

Net at Work Mail Gateway 9.1

Betriebshandbuch

- NoSpamProxy
- enQsig CS
- Large File Transfer



Impressum

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn

Handelsmarken

07.08.2014

Inhalt

1. Das Net at Work Mail Gateway

NoSpamProxy

Spam und Spam-Schutz

Mit immer ausgefeilteren Methoden versuchen Spammer bestehende Schutzsysteme auszuhebeln und ihre Botschaften an den Adressaten zu bringen. Mit dem täglichen Aufräumen des Posteingangs ist es oft leider nicht getan; Spam bedeutet längst eine gravierende ökonomische Belastung für viele Unternehmen.

Spam wirkt störend auf die Geschäftsprozesse und bindet Mitarbeiter ebenso wie System-Ressourcen. Die ungewünschten E-Mails können zudem Ihre E-Mail-Server erheblich beeinträchtigen und im Extremfall sogar lahm legen. Sie können Inhalte und Anhänge aufweisen, die Ihr System angreifen oder ausspähen und so eine Bedrohung für Ihr Unternehmen darstellen.

Des Weiteren versuchen Spammer gerne Ihr System als Relay zu missbrauchen. Ist dies möglich, dann werden E-Mails unter „Ihrem Namen“ - und auf Kosten Ihrer Kapazität versendet. Die Folge kann sein, dass seriöse E-Mail-Partner Ihre Domäne als Spam-Sender bewerten und wichtige Verbindungen unversehens gesperrt werden.

Nicht nur die Angriffs-Szenarien sind vielfältig und komplex; hinzukommt, dass Spam nicht immer gleich Spam ist. So verschieden die Interessen von Unternehmen sein können, so unterschiedlich kann die Bewertung einer E-Mail ausfallen. Ob Sie eine E-Mail-Werbung, einen Newsletter oder eine E-Mail mit chinesischen Schriftzeichen als Spam einstufen, sollten Sie selbst definieren können. Und genau dies ermöglicht Ihnen das Net at Work Mail Gateway mit NoSpamProxy.

Abwehren statt Sortieren

Viele Spammer reagieren immer schneller und versierter auf neue Schutzmethoden. Dies bedeutet, dass statische Spam-Filter kurzfristig mitunter sehr erfolgreich arbeiten - und dennoch morgen schon nutzlos sein können.

Ein effektiver Spam-Schutz muss daher intelligent, flexibel und lernfähig sein, um wirklich zu greifen.

Er sollte nicht nur vor unerwünschten E-Mails schützen. Mindestens genauso wichtig ist es, dass er „gute“ E-Mails korrekt bewertet. Eine Quote von 98 % geblockter Spam-E-Mails klingt gut - nur schadet sie mehr als sie nützt, wenn dabei wichtige gute E-Mails versehentlich mitgeblockt werden oder im falschen Ordner landen. Außerdem sollte der Schutz genauso individuell und vielseitig sein, wie es die Anforderungen Ihrer Geschäftsprozesse sind. Gleichgültig, ob Ihr Unternehmen 25 oder 5.000 Mitarbeiter hat. Letztendlich sollte ein Schutz Ihr System und die Unternehmensabläufe nicht nur vor Spam bewahren, sondern auch vor unnützer Belastung des Systems - denn die Schonung Ihrer Ressourcen steht schließlich im Mittelpunkt.

Diese Anforderungen an einen intelligenten Spam-Schutz waren unser Antrieb zur Entwicklung von NoSpamProxy. Der Grundgedanke ist einfach: Im Gegensatz zu anderen Filtern wehrt NoSpamProxy Spam-E-Mails ab, bevor sie in Ihr System gelangen. Strikt nach dem Motto: Abwehren statt Sortieren.

Wie kann ich als Anwender einen False Positive korrigieren?

Als False Positives bezeichnet man gute E-Mails, die versehentlich als verdächtig bewertet und abgelehnt werden. Wie bereits erwähnt, liegt hierin eine der größten Gefahren einer Filterlösung: Je mehr Spam Sie aussortieren müssen, desto wahrscheinlicher ist es, dass Sie versehentlich eine gute E-Mail beseitigen. Die Folgen können unter Umständen fatal sein.

Angenommen Sie erhalten von einem Kunden per Telefon die Nachricht, dass seine E-Mail an Sie nicht durchgekommen ist, sondern als Spam klassifiziert und abgewiesen wurde. Diese unschöne Situation können Sie mit NoSpamProxy auf einem einfachen Weg auflösen. Sie brauchen hierzu kein Administrator zu sein und keine Einstellungen am System vorzunehmen oder an NoSpamProxy etwas zu ändern; schicken Sie einfach Ihrerseits eine E-Mail an den Kunden.

Die nächste E-Mail des Kunden wird dann von NoSpamProxy automatisch als Reaktion auf Ihre E-Mail gewertet - auch wenn der Absender nicht die „Antwort“-Funktion verwendet - und als gut bzw. erwünscht beurteilt.

Dies bedeutet, dass ein zweiter Anlauf in der Regel problemlos durchkommt und keine weiteren False Positives entstehen. Die E-Mail-Adresse des Absenders ist von NoSpamProxy als vertrauenswürdig eingestuft worden.

Proxy statt Relay

NoSpamProxy ist, wie der Name schon sagt, als Proxy konzipiert. Vereinfacht gesagt ist ein Proxy eine Zwischenstation zwischen dem Internet und Ihrem System. Ähnlich wie bei einer Firewall ist Ihr internes Netzwerk vor einem ungefilterten Kontakt mit dem Internet geschützt.

Bei einer eingehenden E-Mail wird zunächst eine Verbindung von außen zu NoSpamProxy aufgebaut. Anschließend stellt NoSpamProxy eine zweite Verbindung zu Ihrem E-Mail-Server her.

NoSpamProxy protokolliert die Daten mit, extrahiert die relevanten SMTP-Informationen und baut daraus die E-Mail wieder zusammen. Diese E-Mail wird den konfigurierten Filtern zur Prüfung vorgelegt. Wird eine E-Mail als Spam erkannt, verweigert NoSpamProxy die Annahme der E-Mail. Dies veranlasst den einliefernden E-Mail-Server eine Unzustellbarkeitsnachricht an den Absender zu schicken. Ein Proxy ist ideal geeignet, um eine frühzeitige Spam-Abwehr zu realisieren.

Proxy-Vorteile

Viele Funktionen des internen E-Mail-Servers bleiben nutzbar. Zum Beispiel kann der interne E-Mail-Server weiterhin eine E-Mail aufgrund eines vollen oder nicht mehr existierenden Postfachs ablehnen. NoSpamProxy lehnt dann seinerseits die Verbindung von extern ab.

Ihr System wird nicht mit unnützem Datenvolumen beladen. Viele Verbindungen können sehr früh als Spam erkannt werden und belasten den internen E-Mail-Server nicht.

Schutzfunktion

Ihr Server ist nicht von außen erreichbar. Denial of Service-Attacken behindern daher nicht die interne Kommunikation.

enQsig CS

Die Anbindung an das De-Mail-System ermöglicht das Versenden von De-Mails, als wären es ganz normale E-Mails. Für die Anbindung an weitere Systeme wie dem E-Postbrief, der Deutschland-Online - Infrastruktur sowie POP3-Postfächern können Sie die enQsig CS ebenfalls nutzen. Die Connector Services sind sowohl in enQsig als auch in enQsig CS verfügbar.

Large File Transfer

Mit dem Large File Transfer können Benutzer über ihre gewohnte Outlook-Oberfläche beliebig große Dateien an Empfänger übertragen, ohne das E-Mail-System belasten zu müssen. Anstatt der Datei selbst wird ein Link an die E-Mail angehängt, mit dessen Hilfe der oder die Empfänger der E-Mail die Dateien über SSL abgesichert herunterladen können. Zusätzlich können Sie externen Empfängern auch einen Einladungslink für das Web Portal des Large File Transfer zusenden, damit diese große Dateien Ihnen zusenden können.



Sprechen Sie uns unter info@netatwork.de an, wenn Sie die Möglichkeiten des Large File Transfer interessieren. Wir beraten Sie gerne und unterstützen Sie bei der Erweiterung Ihrer bestehenden Lizenz.

Mehrnutzen durch zentrale Verschlüsselung und digitale Signatur

Da enQsig auf den Technologien des bewährten Anti-Spam-Gateways NoSpamProxy basiert, lassen sich dessen Funktionen einfach durch eine Lizenzerweiterung freischalten. So kann auf nur einem Gateway und mit einer einheitlichen Administration die vertrauliche Kommunikation mit Partnern durchgeführt werden.

2. Die Rollen des Net at Work Mail Gateways

Das Net at Work Mail Gateway besteht aus mehreren Rollen, die im Weiteren beschrieben werden.

Gateway Rolle

Hinter der Gateway Rolle verbirgt sich der eigentliche Kern des Net at Work Mail Gateways. In Abhängigkeit von Ihrer Umgebung kann diese Rolle entweder in eine Demilitarisierte Zone (DMZ) oder im Intranet installiert werden. Um ein hochverfügbares System aufzubauen, kann diese Rolle auf mehreren Servern installiert werden.

NoSpamProxy nimmt die E-Mails auf Port 25 an, prüft auf Spam und weist sie gegebenenfalls ab.

Die Connector Services von enQsig CS stellen eine Schnittstelle zu De-Mail, E-Postbrief, Deutschland-Online - Infrastruktur und POP3-Postfächern bereit.

Intranet Rolle

Wie der Namen schon andeutet, wird die Intranet Rolle typischerweise im Intranet Ihres Unternehmens installiert.

Web Portal

Wenn Sie den Large File Transfer aktiviert haben, können Anwender große Dateien über das Web Portal übertragen.

Um ein hochverfügbares System aufzubauen, kann diese Rolle auf mehreren Servern installiert werden.

3. Funktionsweise und Einbindung in die Infrastruktur

Das Net at Work Mail Gateway arbeitet in Ihrer Umgebung mit den anderen Komponenten Ihrer Infrastruktur zusammen (Bild 1).

Alle Komponenten des Systems können auf demselben Server betrieben werden. Das Net at Work Mail Gateway kann in kleinen Umgebungen zusammen mit einer Firewall und Ihrem E-Mail-Server auf einem einzigen Server installiert werden. Zusätzlich zu den einzelnen Komponenten sind auch die TCP Ports dokumentiert, die zwischen den Komponenten verwendet werden (Bild 2).

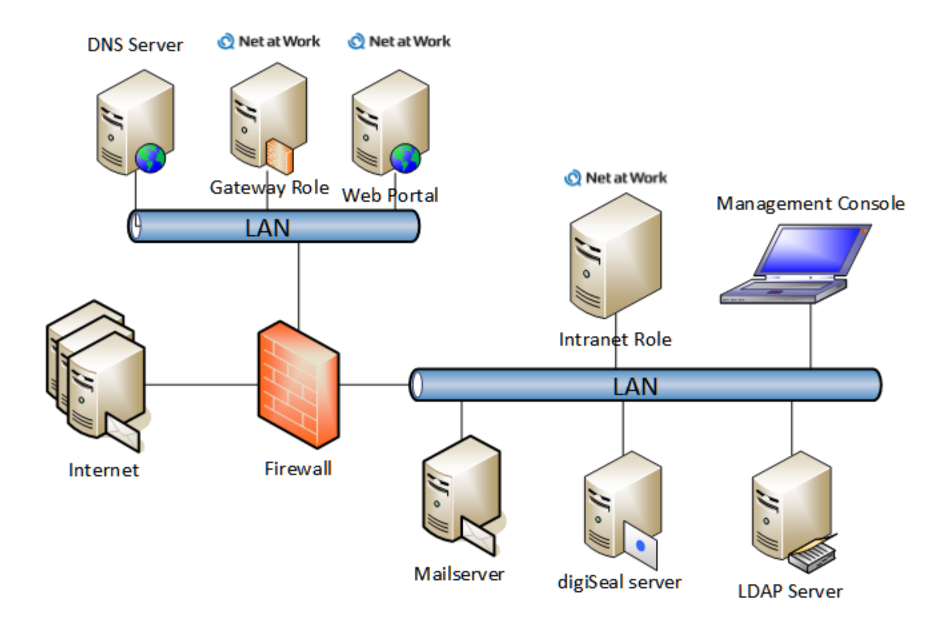


Bild 1: Komponenten des Net at Work Mail Gateways

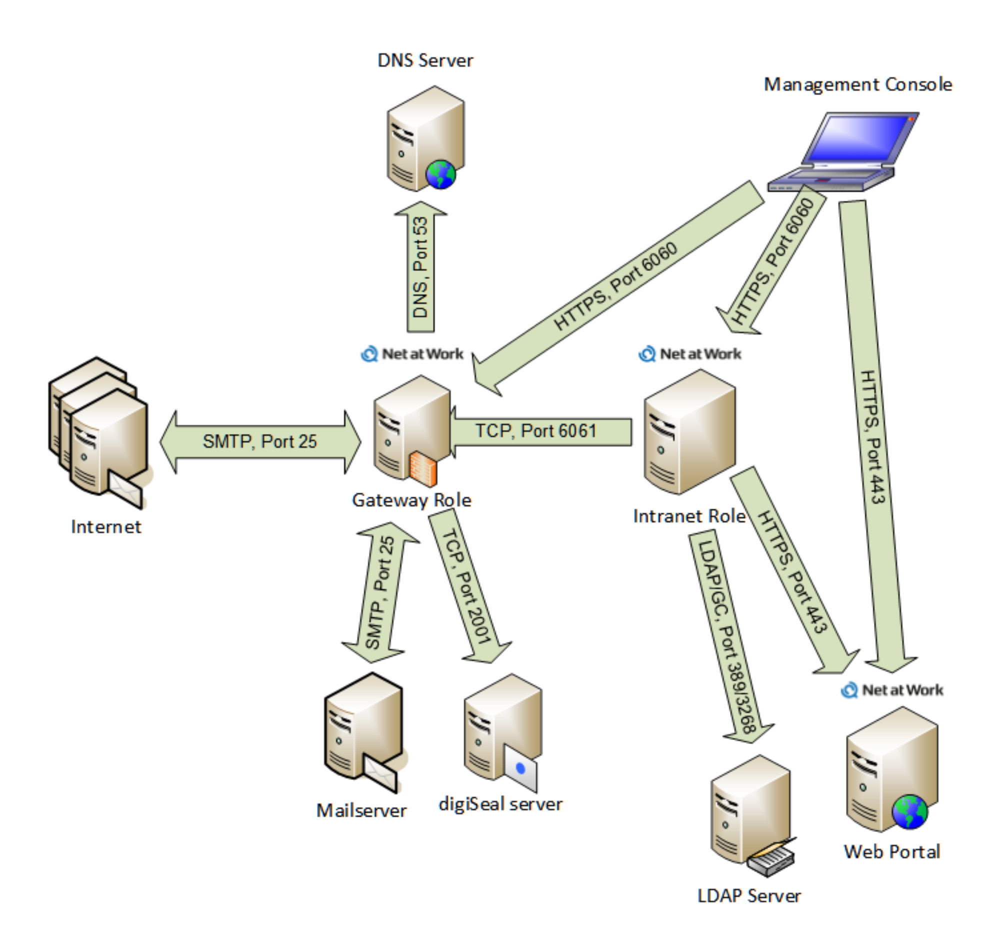


Bild 2: Kommunikation des Net at Work Mail Gateways untereinander und mit anderen Komponenten

Firewall

Für die Funktion des Net at Work Mail Gateways ist es erforderlich, dass das Netzwerk die nötigen Kommunikationsbeziehungen nicht verhindert. Dies ist im Wesentlichen das Protokoll SMTP auf Port 25/TCP und DNS auf Port 53 TCP/UDP. Sofern die Rollen des Net at Work Mail Gateways in unterschiedlichen Netzwerksegmenten installiert werden, muss auf der Firewall die Kommunikation für TCP auf Port 6060 und 6061 erlaubt werden. Sowohl die Management Konsole als auf die Intranet Rolle verwenden Port 443/HTTPS um auf das Web Portal zuzugreifen.

SMTP E-Mail-Server

Die Vorgehensweise des Net at Work Mail Gateways basiert auf der Zustellung der E-Mails über das Standardprotokoll SMTP. Ein unverzichtbarer Bestandteil des Systems ist daher ein SMTP E-Mail-Server, an den das Gateway die eingehenden E-Mails weiterleiten kann.

Die ausgehenden E-Mails sollten auch über das Net at Work Mail Gateway versandt werden, damit das Level-of-Trust-System die Kommunikationsbeziehungen Ihrer Organisation erlernen kann.

SQL-Datenbank

Das Net at Work Mail Gateway speichert seine Daten, die es zum Betrieb benötigt, in einer Microsoft SQL Datenbank. Das Gateway unterstützt dabei den Microsoft SQL Server 2005 oder neuer. Die kostenlose Express Edition kann verwendet werden.

Domain Name System (DNS)

Ihr System sollte über eine Domain Name System (DNS)-Auflösung verfügen. Es gehört zum guten Ton, dass der DNS-Name, mit dem sich ein E-Mail-Server meldet auch per DNS auflösbar ist. Meldet sich ein Server als „mail.netatwork.de“, sollte er auch als „mail.netatwork.de“ im DNS auflösbar sein. Ist er nicht auflösbar, dann ist der Domain-Name entweder falsch, was auf eine Fehlkonfiguration des DNS Servers hindeutet, oder der DNS Name ist nicht im DNS gepflegt.

Verzeichnisdienst, Active Directory

Das Net at Work Mail Gateway kann E-Mails an nicht existierende oder nicht berechtigte Empfänger schon beim Empfang ablehnen. Dazu muss im Gateway eine Liste der gültigen SMTP-Adressen gepflegt werden. Dies kann z.B. über einen automatischen Abgleich mit den Daten aus dem Active Directory oder Lotus Domino erfolgen. Wenn Sie dies nicht wünschen, können Sie die Benutzer auch manuell einpflegen.

Beispiele für die Implementierung

Prinzipielles zum Einsatz des Net at Work Mail Gateways

Ob die E-Mail von einem Provider oder direkt vom Absender kommt: Das Net at Work Mail Gateway steht an „vorderster Front“ vor dem ersten E-Mail-Server oder Relay des Empfängers.

Ist dies nicht der Fall, so kann in diesem Fall weder die IP-Adresse des einliefernden Gateways geprüft, noch die Verbindung mit einer Fehlermeldung abgebrochen werden. Das einliefernde Gateway würde eine Unzustellbarkeitsnachricht versenden. Der wesentliche Vorteil des Net at Work Mail Gateways, E-Mails abzulehnen und Datenvolumen zu sparen, würde nicht greifen.

Net at Work Mail Gateway vorgeschaltet

Die einfachste Funktion ist die Vorschaltung vom Net at Work Mail Gateway als eigenes System vor den eigenen E-Mail-Server (Bild 3).

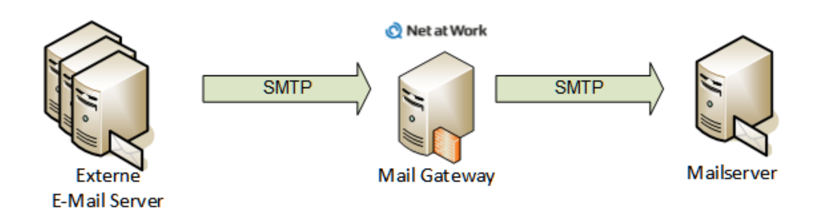


Bild 3: Das Net at Work Mail Gateway vor dem eigenen E-Mail-Server

Net at Work Mail Gateway auf dem E-Mail-Server

Für kleine Umgebung ist es unter Umständen zu aufwändig einen eigenen Server für das Net at Work Mail Gateway zur Verfügung zu stellen. In diesem Fall kann das Gateway auf dem bestehenden E-Mail-Server installiert werden.

In diesem Fall ändern Sie die Konfiguration des bestehenden E-Mail-Servers wie folgt: Anstatt eingehende E-Mails auf Port 25 anzunehmen, konfigurieren Sie hierfür einen anderen Port (z.B. 2525). Anschließend konfigurieren Sie im Net at Work Mail Gateway einen Smarthost für eingehende E-Mails für Host localhost, Port 2525.

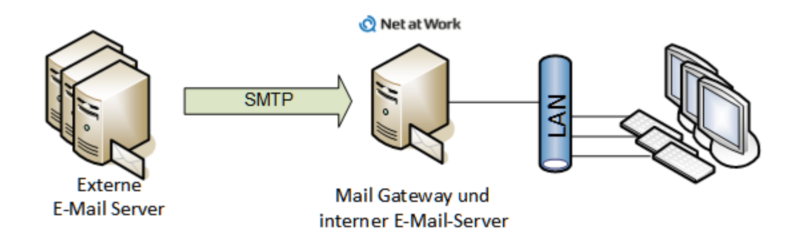


Bild 4: Das Net at Work Mail Gateway auf dem E-Mail-Server

Das Net at Work Mail Gateway nimmt nun die Verbindungen auf Port 25 an und leitet diese dann an den E-Mail-Server über „localhost:neuerPort“ weiter.

Net at Work Mail Gateway mit NAT-Router

Wenn der Server selbst nicht über eine eigene offizielle IP-Adresse verfügt, dann ist ein System vor dem Server für die Umsetzung zuständig. Bei kleineren Installationen ist dies meist ein Router mit Network Address Translation (NAT).

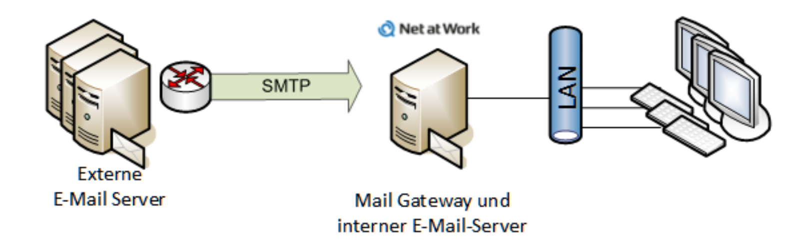


Bild 5: Net at Work Mail Gateway mit NAT Router

Diesen müssen Sie für den Einsatz mit dem Net at Work Mail Gateway so einstellen, dass er alle Verbindungen, die auf die offizielle IP-Adresse an Port 25 ankommen, an das Net at Work Mail Gateway weitergibt. Die Konfiguration des Gateways entspricht dabei einem der beiden vorherigen Beispiele.

Das Net at Work Mail Gateway mit Firewall und DMZ

Größere Installationen nutzen häufig eine mehrstufige Firewall oder eine so genannte „Demilitarisierte Zone“ (DMZ), um den Datenverkehr zwischen den Systemen besser kontrollieren zu können.

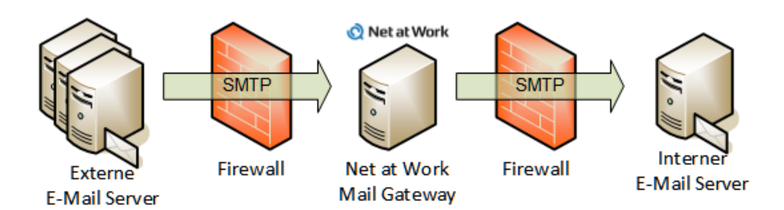


Bild 6: Net at Work Mail Gateway mit Firewall

In diesem Fall ist das Net at Work Mail Gateway auf einem eigenen Server in der DMZ installiert. Die Firewall lässt Verbindungen von außen auf den Server, an Port 25 des Net at Work Mail Gateways, zu. Bei dieser Konstellation sollten Sie nur die Gateway Rolle in der DMZ installieren. Die Intranet Rolle sollten Sie im Intranet installieren.

Das Net at Work Mail Gateway und SMTP-Virenscanner

Das Net at Work Mail Gateway mit NoSpamProxy kann, mit einem vorhandenen Virenscanner, selbst E-Mails auf Viren prüfen. Wenn Sie weiter Ihren bisherigen SMTP-Virenscanner auf dem Transportweg nutzen möchten, müssen Sie darauf achten, dass dieser zwischen NoSpamProxy und dem internen E-Mail-Server eingebunden wird.

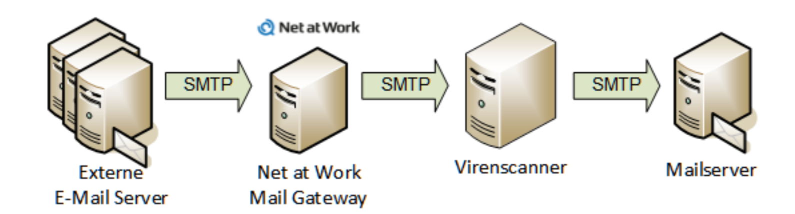


Bild 7: NoSpamProxy mit Virenscanner



Ein SMTP-Virenscanner arbeitet in der Regel als SMTP-Relay und darf daher nicht zwischen Internet und NoSpamProxy eingebunden werden.

Installation der Rollen auf unterschiedlichen Servern

In sehr kleinen Umgebungen empfiehlt es sich, alle Rollen auf einem Server zu installieren. Auch auf einem Small Business Server läuft das Net at Work Mail Gateway ohne Einschränkungen.

In größeren Umgebungen mit einer DMZ könnte eine mögliche Verteilung der Rollen wie im folgenden Diagramm aussehen (Bild 8).

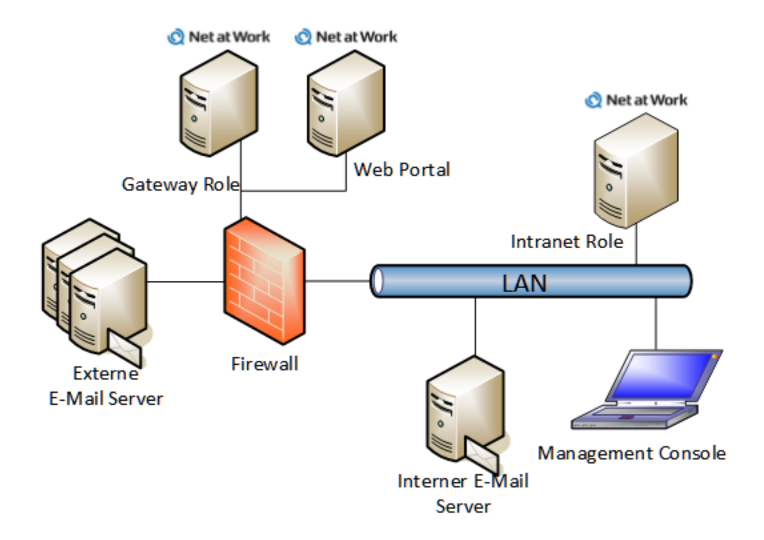


Bild 8: Installation des Net at Work Mail Gateways in der DMZ

In der Demilitarisierten Zone (DMZ) steht ein Server mit der installierten Gateway Rolle. Hier werden die E-Mails verarbeitet, gefiltert und anschließend an den internen E-Mail-Server weitergeleitet. Im LAN könnte dann ein Server laufen, auf dem die Intranet Rolle installiert sind. Der Vorteil dieser Vorgehensweise ist bei den Sicherheitsaspekten zu suchen. Auf der Firewall müssen für den Datentransfer zwischen der Gateway Rolle und den anderen beiden Rollen lediglich die Ports 6060 und 6061 aus dem LAN in die DMZ geöffnet werden. Die einzige zwingende Verbindung aus der DMZ in das LAN ist der Port 25 für die E-Mail-Kommunikation.

In größeren Umgebungen mit hohem E-Mail-Aufkommen haben Sie die Möglichkeit in der DMZ mehrere Server mit der Gateway Rolle zu installieren. Hiermit es möglich, ein hochverfügbares System aufzubauen. Auf dem PC des Administrators kann man die Net-at-Work-Mail-Gateway-Verwaltungskonsole installieren und damit alle anderen Rollen im LAN und in der DMZ zentral verwalten (Bild 9).

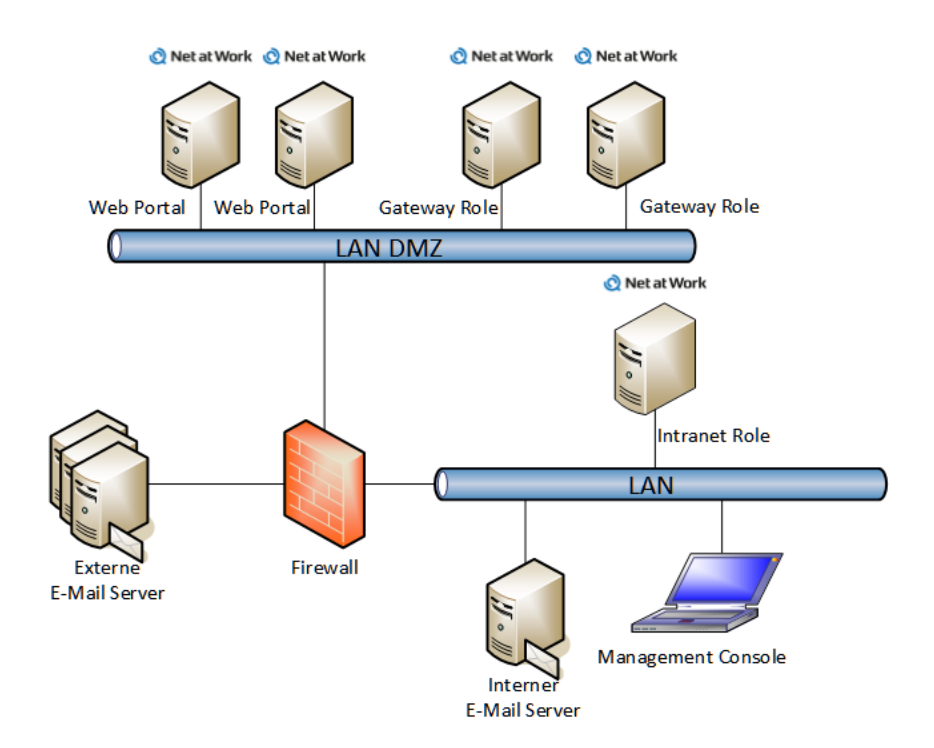


Bild 9: Rollen des Net at Work Mail Gateways auf verteilten Servern

Negativbeispiel: Falsche Konfiguration

Zur Verdeutlichung zeigt dieses Bild eine nicht zulässige Installation.

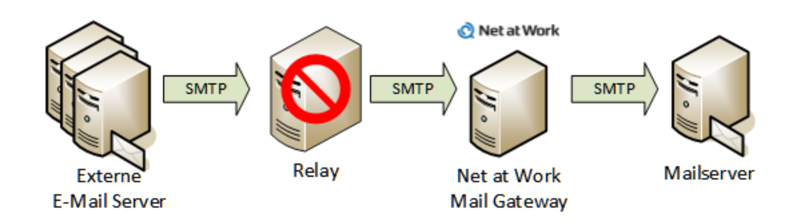


Bild 10: Falsche Konfiguration - das Net at Work Mail Gateway mit NoSpamProxy kann nicht funktionieren

Wie bereits angesprochen: Eine eingehende E-Mail wird durch das Relay schon komplett empfangen, bevor sie an NoSpamProxy gesendet wird. Resultat: NoSpamProxy kann nicht sinnvoll arbeiten. Weder wird Datenvolumen eingespart, noch kann NoSpamProxy eine bestehende Verbindung abbrechen. Es wäre auch unmöglich, die IP-Adresse des eingehenden Gateway zu prüfen.

Ausgehende E-Mails

Der Erfolg des Level-of-Trust-Systems hängt im großen Maß davon ab, dass ausgehende E-Mails über das Net at Work Mail Gateway versandt werden.

Das Net at Work Mail Gateway kann sich bei ausgehenden E-Mails eines Smarthosts bedienen oder die E-Mails direkt zustellen. Sie können beim Versand über einen weiteren Smarthost, z. B. den Smarthost Ihres Providers nehmen, oder ein eigens für den Versand installiertes Mail-Relay. Welche Variante Sie nutzen, ist Ihnen überlassen.



Wenn Sie nicht über eine statische IP-Adresse verfügen, dann sollten Sie ausgehende E-Mails über Ihren Provider schicken. Dynamische IP-Adressen werden von vielen Firmen und E-Mail-Providern kategorisch abgelehnt.

4. Net at Work Mail Gateway Verwaltungskonsole

Das Net at Work Mail Gateway wird über eine Microsoft Management Console (MMC) verwaltet. Die Installation der Oberfläche wird in der Net at Work Mail Gateway Installationsanleitung beschrieben. Bitte beachten Sie die Hinweise in diesem Handbuch vor dem Inbetriebnehmen des Net at Work Mail Gateways.

Die Verwaltungskonsole des Gateways gliedert sich in folgenden Bereiche:

- **Die Übersichtsseite**
  Unter dem Obersten Knoten der Verwaltungskonsole mit dem Namen **Net at Work Mail Gateway** liegt die Übersichtsseite. Sie bietet einen schnellen Überblick über das gesamte Gateway mit allen verbundenen Rollen. Sie können außerdem auf dieser Seite auch verschieden Aktionen starten, die im Kapitel der Übersichtsseite beschrieben werden.
- **Monitoring**
  Das **Monitoring** bietet eine Übersicht über den Empfang und die Zustellung von E-Mails. Zusätzlich können Sie die Ereignisanzeige von allen verbundenen Servern des Net at Work Mail Gateway einsehen.
- **Menschen und Identitäten**
  Der Bereich **Menschen und Identitäten** verwaltet Ihre eigenen Domänen und lokalen Benutzer aber auch externe Kommunikationspartner. Sie können für diese Identitäten Einstellungen zu Vertrauen und Sicherheit festlegen.
- **Konfiguration**
  Die Knoten unter **Konfiguration** dienen der Einstellung Ihres Net at Work Mail Gateway. Hier definieren Sie Sende- und Empfangskonnektoren für E-Mails, Ihre Regeln und Benachrichtigungen aber auch die Verbindungen zu Komponenten des Net at Work Mail Gateways oder Drittanbieterkomponenten.
- **Troubleshooting**
  Zur Diagnose des Net at Work Mail Gateways steht Ihnen der Bereich **Troubleshooting** zur Verfügung. Erstellen Sie Logs der einzelnen Gateway Komponenten oder lassen Sie Einstellungen automatisch korrigieren.

Sprache der Oberfläche ändern

Die Oberfläche des Net at Work Mail Gateway ist standardmäßig auf die Systemsprache eingestellt. Wenn Sie die Sprache ändern möchten, klicken Sie auf den Knoten **Net at Work Mail Gateway** und wählen Sie im Menü **Aktion** / **Sprache ändern** bzw. **Action** / **Change language**. Alternativ können Sie diese Funktion durch einen Rechtsklick auf dem Knoten **Net at Work Mail Gateway** anwählen. Damit die Änderung wirksam wird, müssen Sie die Oberfläche schließen und neu starten.

Verbindung zur Intranet Rolle herstellen

Die Verbindung der Management Konsole zur Intranet Rolle steht nach der Installation auf `localhost`. Bei einer Installation der Konsole auf einem anderen Rechner als der Rechner der Intranet Rolle müssen Sie die Verbindung anpassen. Bitte wählen Sie dazu im Menü **Aktion** / **Server ändern** bzw. **Action** / **Change server**. Geben Sie hier den Namen des Servers (zum Beispiel: „mail.example.com“) und den Port (normalerweise „6060“) ein. Alternativ können Sie auch diese Funktion durch einen Rechtsklick auf

dem Knoten **Net at Work Mail Gateway** anwählen. Damit die Änderung wirksam wird, müssen Sie die Oberfläche schließen und neu starten.



Falls das Gateway in einer DMZ betrieben wird und Sie aus dem LAN mit der Net at Work Mail Gateway MMC den Dienst fernsteuern möchten, müssen Sie auf der Firewall lediglich den TCP-Port 6060 freischalten. Diese Verbindung ist zertifikatsbasierend verschlüsselt.

5. Übersichtsseite

Die Seite unter dem Knoten **Net at Work Mail Gateway** (Bild 11) dient Ihrem schnellen Überblick. Sie erhalten hier eine Übersicht über den Status der installierten Rollen.

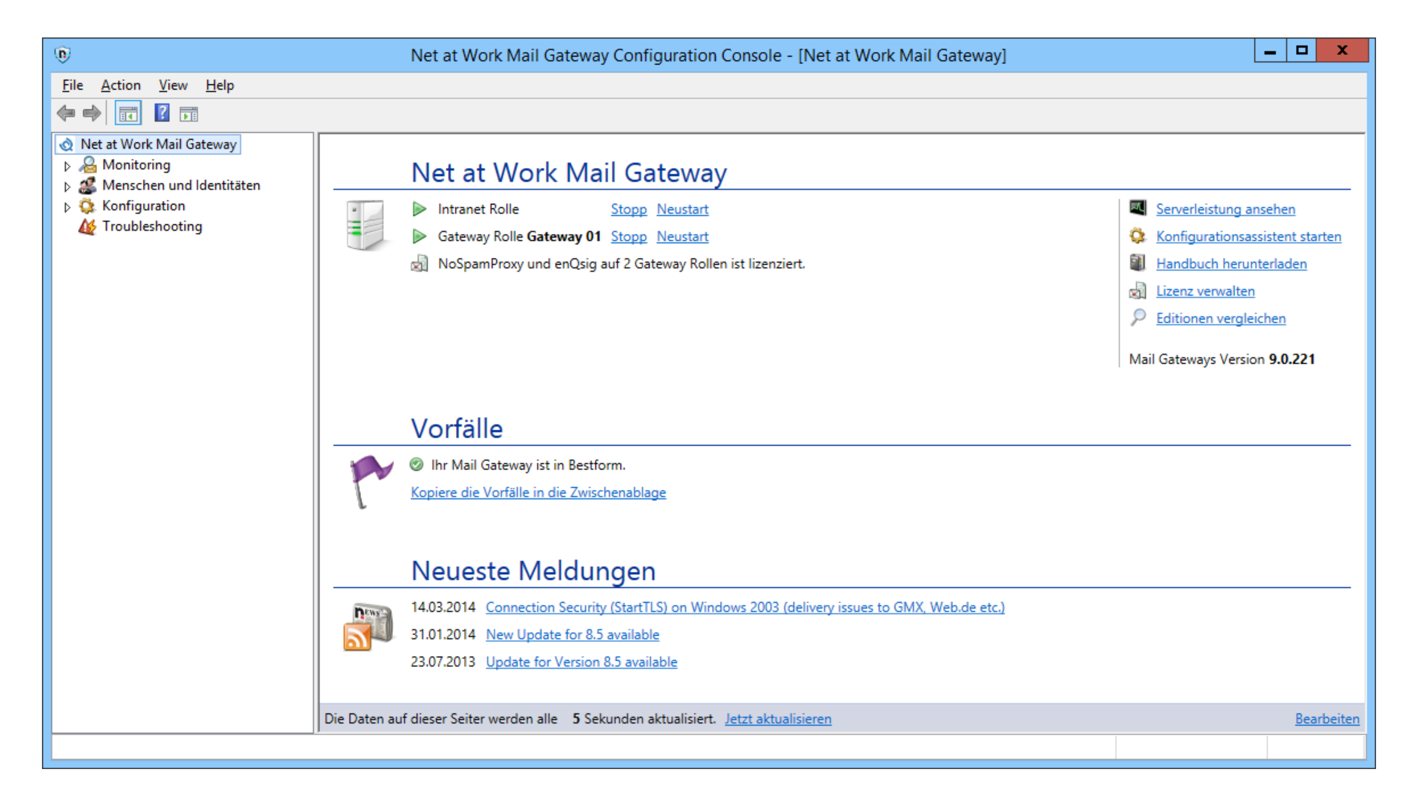


Bild 11: Die Übersicht über die Konfiguration der Gateway Rolle

Bei der ersten Inbetriebnahme ist das Net at Work Mail Gateway weitgehend unkonfiguriert. Die fehlenden Konfigurationsoptionen erscheinen in der Liste **Vorfälle**. Statt jeden Vorfall einzeln abzuarbeiten, empfehlen wir die Verwendung des Konfigurationsassistenten. Der Assistent unterstützt Sie bei der schnellen und vollständigen Inbetriebnahme des Gateways in den meisten Umgebungen. Er ermittelt und erstellt anhand der lizenzierten Funktionen in Ihrer Lizenz die empfohlene Konfiguration.

Liste der Rollen

Direkt unter der Überschrift **Net at Work Mail Gateway** werden alle verbunden Rollen aufgeführt. Die Liste zeigt für jede Rolle an, ob Sie gestartet oder gestoppt ist. Zusätzlich können Sie die Rollen auch manuell starten und stoppen. Unter der Liste wird nach dem einspielen der Lizenz eine Zusammenfassung der Lizenz angezeigt

Bereich für Aktionen

In der rechten oberen Ecke werden die derzeit möglichen Aktionen angezeigt. Unter der Liste mit den Aktionen steht die installierte Version des Net at Work Mail Gateways.

Serverleistung ansehen

Die Aktion **Serverleistung ansehen** gibt Ihnen einen schnellen Überblick über die aktuelle Verarbeitung von E-Mails und die derzeit zu Verfügung stehenden Ressourcen.

Datenverkehr

Die Seite **Datenverkehr** zeigt einen gleitenden Durchschnitt der verarbeiteten E-Mails der letzten Minute bzw. Stunde. Die Seite wird automatisch aktualisiert und zeigt dadurch ob Ihr Mail Gateway aktuell E-Mail empfängt (Bild 12).

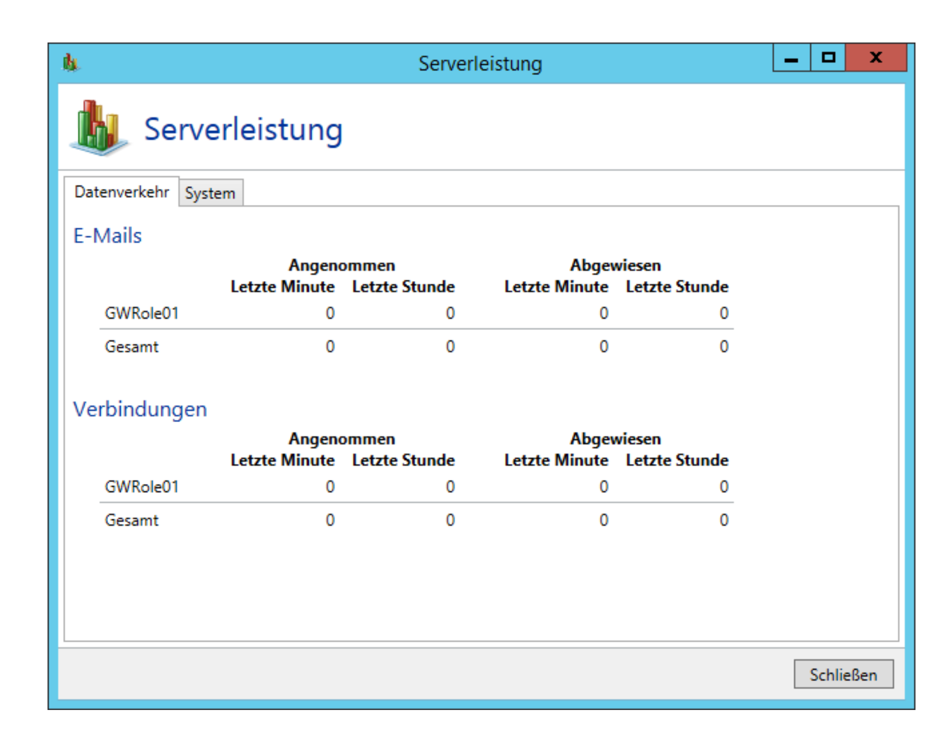


Bild 12: Die aktuell verarbeiteten Nachrichten

System

Die Seite **System** zeigt für jedes System mit Intranet oder Gateway Rollen die installierten Dienste, deren Status und die verwendeten Ressourcen (Bild 12).

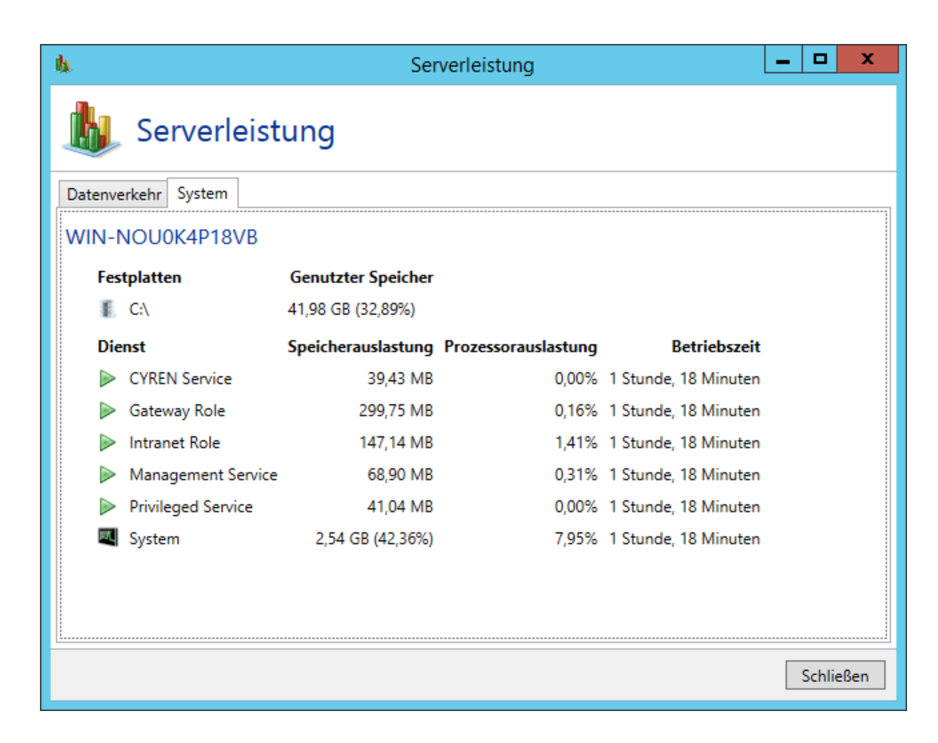


Bild 13: Die zur verwendeten und zur Verfügung stehenden Ressourcen

Zusätzlich zu dieser Ansicht stehen Ihnen auf dem Server außerdem die Leistungsindikatoren zur Verfügung.

Konfigurationsassistent starten

Der Eintrag **Konfigurationsassistent starten** führt Sie durch alle wesentlichen Schritte einer Mail Gateway Konfiguration, um die ordnungsgemäße Funktionsweise sicherzustellen.

Der Konfigurationsassistent führt Sie durch folgende Konfigurationen:

- **Lizenz**
  Spielen Sie eine Lizenz ein oder ändern Sie die bestehende Lizenz. Falls Sie noch keine Regeln erstellt haben können Sie in Abhängigkeit von Ihren lizenzierten Funktionen die passenden Standardregeln erstellen lassen.
- **Verbindung zur Gateway Rolle**
  Wenn noch keine Gateway Rolle verbunden wurde, können Sie hier Ihre Gateway Rolle verbinden. Nach dem Hinzufügen der Rolle legen Sie bitte noch den DNS Namens für die Server-Identität dieser Gateway Rolle fest.
- **Eigene Domänen**
  Konfiguration der eigenen Domänen. Falls das Gateway beim Ausführen des Assistenten noch keine eigenen Domänen eingetragen hat, wird in diesem Schritt die primäre Domäne der Lizenz in die Liste der eigenen Domänen eingefügt.
- **Interne E-Mail-Server**
  Konfiguration der internen E-Mail-Server.
- **Eingehende Zustellung**

Konfiguration der eingehenden Zustellung von E-Mails an den internen E-Mail-Server.

- **Ausgehende Zustellung**
  Konfiguration der ausgehenden Zustellung von E-Mails an externe E-Mail-Server.
- **Administrative E-Mail-Adressen**
  Konfigurieren Sie die administrativen E-Mail-Adressen.
- **Schutz sensibler Daten**
  Legen Sie ein Passwort zum Schutz sensibler Daten fest.

Nach Abschluss des Assistenten führen Sie bitte noch eine Kontrolle durch:

- Kontrollieren Sie die Konfiguration der Empfangskonnektoren.

Die Durchführung dieser Schritte stellt die Funktion des Net at Work Mail Gateway sicher.

Handbuch herunterladen

Über diese Aktion laden Sie das aktuelle Benutzerhandbuch herunter. Wenn Sie bereits Ihre Lizenz in das Mail Gateway eingespielt haben, wird die für Ihre Lizenz passende Version des Handbuchs heruntergeladen.

Lizenz verwalten

Die Aktion öffnet den Dialog für die derzeit verwendete Lizenz. Er zeigt Ihnen alle relevanten Daten Ihrer Lizenz und warnt Sie, falls Probleme mit der Lizenz auftreten (Bild 14).

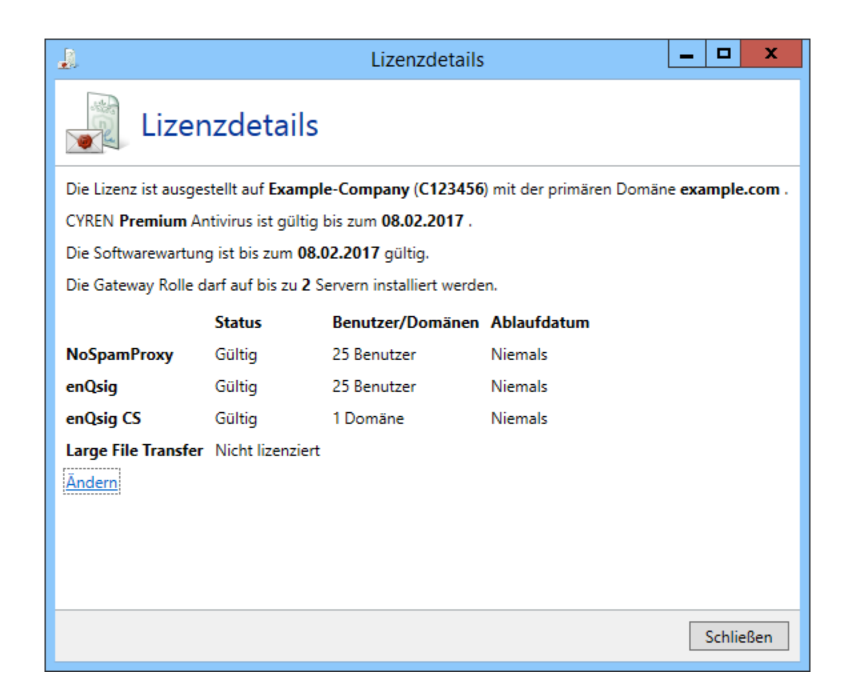


Bild 14: Die derzeitig eingespielte Lizenz

Sie sehen hier Ihre C-Nummer und Domäne alle lizenzierten Funktionen Information und deren Gültigkeitszeitraum. Durch den Link **Ändern** können Sie eine andere Lizenz-Datei laden und im Mail Gateway verwenden, soweit das Ablaufdatum der Softwarewartung noch mindestens genau so weit oder weiter in der Zukunft liegt wie bei der derzeit verwendeten Lizenz.

Editionen vergleichen

Der Link öffnet die Seite mit dem Vergleich der Lizenz-Features. Jede Feature wird hier kurz erklärt.

Update herunterladen

Falls auf dem Server von Net at Work eine neuere Version des Mail Gateways veröffentlicht wurde, wird diese Aktion eingeblendet. Sie laden damit die Installer-Datei des Mail Gateways herunter. Die Installation können Sie im Nachhinein manuell anstoßen.

Vorfälle

Die Liste der **Vorfälle** zeigt Ihnen an, falls Einstellungen fehlen oder fehlerhaft sind, die für den Betrieb des Gateways relevant sind. Wenn zum Beispiel der Weg für die ausgehenden E-Mails noch nicht definiert wurde, werden Sie auf dieser Seite darauf hingewiesen.

Neueste Meldungen

Diese Meldungen weisen Sie auf Produktaktualisierungen oder allgemeine Verbesserungsvorschläge für die Konfiguration des Mail Gateway hin.

6. Monitoring

Die Knoten unterhalb von Monitoring (Bild 15) informieren Sie über den Empfang und Versand Ihrer E-Mails.

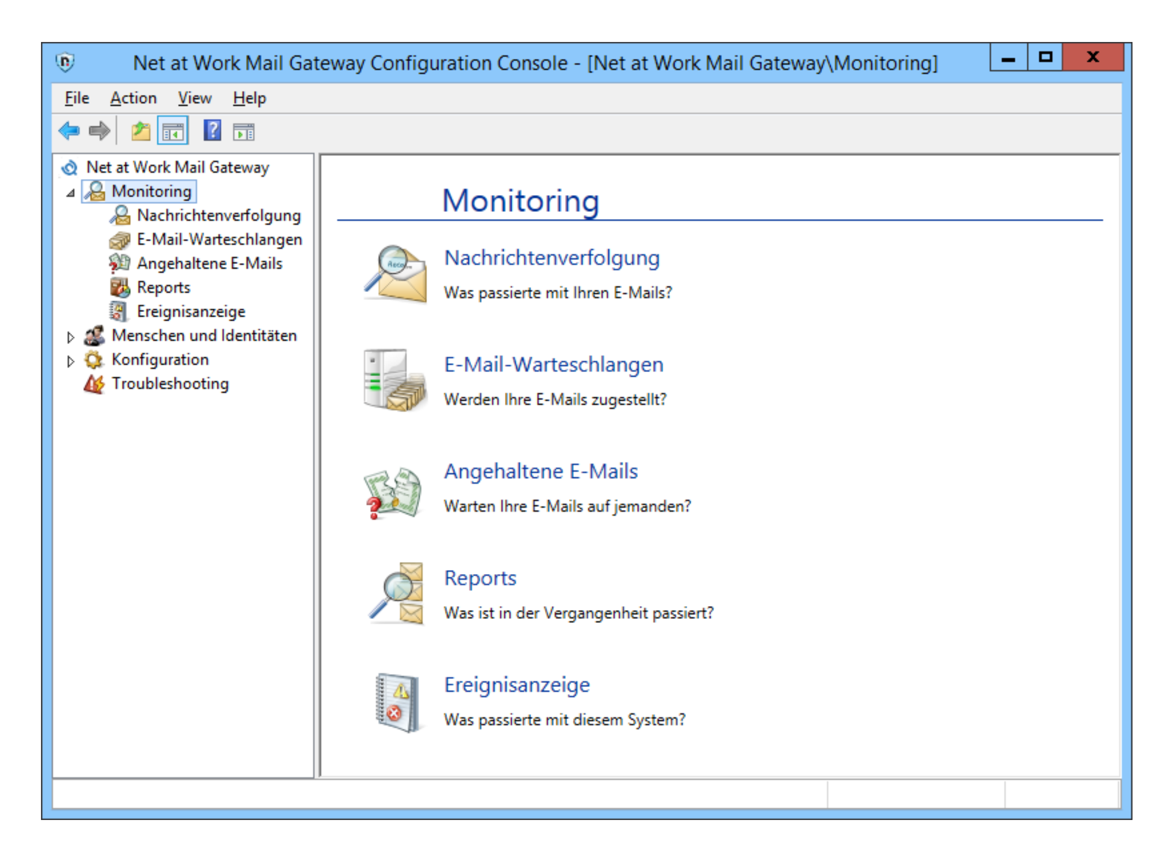


Bild 15: Übersicht über die Bereiche des Monitoring

Nachrichtenverfolgung

Die Nachrichtenverfolgung erlaubt Ihnen nachzuvollziehen, wann welche E-Mails geblockt oder durchgelassen wurden (Bild 16). Die Suche können Sie nach bestimmten Absender- und Empfängerkriterien, dem Betreff sowie nach konkreten Zeitintervallen und dem „E-Mail-Status“ festlegen.

Ferner können Sie die Details nachsehen, wann und was genau mit der E-Mail geschah. So können Sie das Vorgehen des Net at Work Mail Gateways und das Funktionieren der Regeln sehr leicht nachvollziehen.

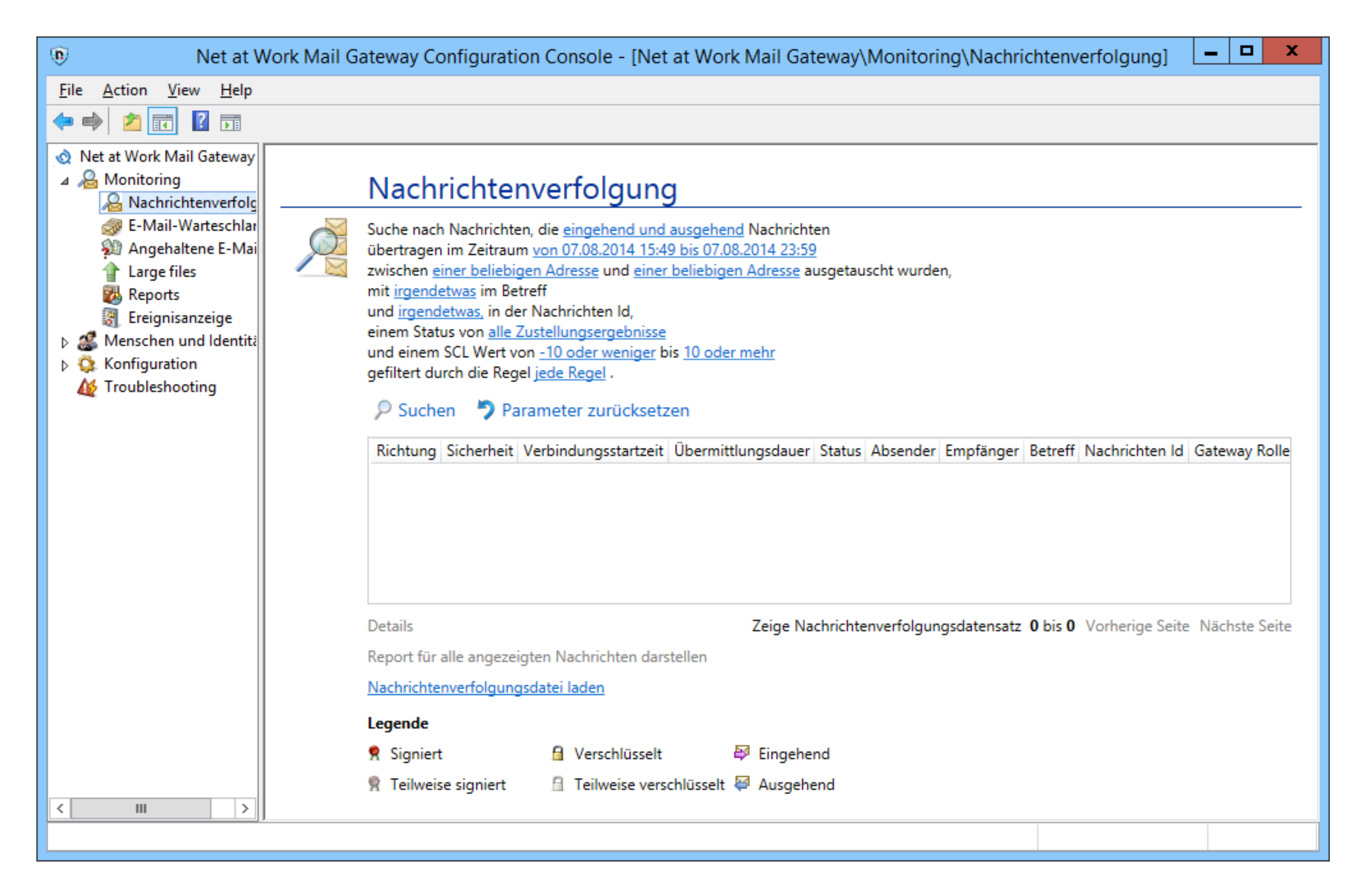


Bild 16: Die Suche der Nachrichtenverfolgungsdatensätze

Um eine E-Mail nachzuverfolgen, haben Sie verschiedene Suchkriterien, die Sie einzeln oder kombiniert anwenden können. Ein Zeitraum, in dem die E-Mail oder die E-Mails eintrafen, muss jedoch in jedem Fall angegeben werden. Standardmäßig wird die Startzeit auf die aktuelle Systemzeit - 1 Stunde und die Endzeit auf heute um 23:59 Uhr gesetzt.

Bei der Suche können Sie auf die folgenden Eigenschaften filtern. Bei der eingabe von Text können Sie immer den gesamten zu suchenden Text eingeben oder Teile davon.

- Richtung: eingehend, ausgehend.
- Versandtzeitraum: Durch die Auswahl unter **Zeiträume** können oft benötigte Suchen schnell gewählt werden.
- Absender- und Empfängeradress: die E-Mail-Adressen der Kommunikationspartner.
- Betreff: Der Inhalt der Betreffzeile.
- Nachrichten Id: Interne Kennung der E-Mail.
- Zustellergebnisse: Der Status der Zustellung.
- SCL Wert: Einschränkung auf den errechneten SCL Wert.
- Regel: Der Name der Regel, von der die Nachricht verarbeitet wurde.

Im der Liste der Nachrichtenverfolgungsdatensätze erscheinen alle E-Mails, die den Suchkriterien entsprechen. Sie werden mit den Angaben **Richtung**, **Sicherheit**, **Verbindungsstartzeit**, **Übermittlungsdauer**, **Status**, **Absender**, **Empfänger**, **Betreff**, **Nachrichten-ID** und **Gateway Rolle** angezeigt.

Die neuesten E-Mails stehen oben in der Liste.

Die Details nachprüfen

In den Details werden Ihnen detaillierte Informationen über den Zustellstatus einer E-Mail dargestellt. Ob und wie eine E-Mail signiert bzw. verschlüsselt wurde, wird hier ebenfalls angezeigt.

Klicken Sie die den Datensatz an, dessen Details Sie einsehen möchten.

Wählen Sie jetzt die Aktion **Nachrichtendetails** oder führen Sie einen Doppelklick aus.

Es erscheint der Dialog **Nachrichtenverfolgung** (Bild 17). Vom Start bis zum Schließen der Verbindung finden Sie hier alle Bearbeitungsschritte und Details, auf Registerkarten verteilt, detailliert aufgeführt. Sie sehen auf einen Blick, ob die Verbindung verschlüsselt wurde und welches Zertifikat der SMTP-Server bzw. der SMTP-Client verwendet hat. Auf den weiteren Registerkarten werden Ihnen die Filterergebnisse und generelle Verarbeitungsfehler vom Net at Work Mail Gateway angezeigt, so dass Sie jederzeit genau nachverfolgen können, ob etwas mit der E-Mail-Zustellung nicht ordnungsgemäß funktioniert.

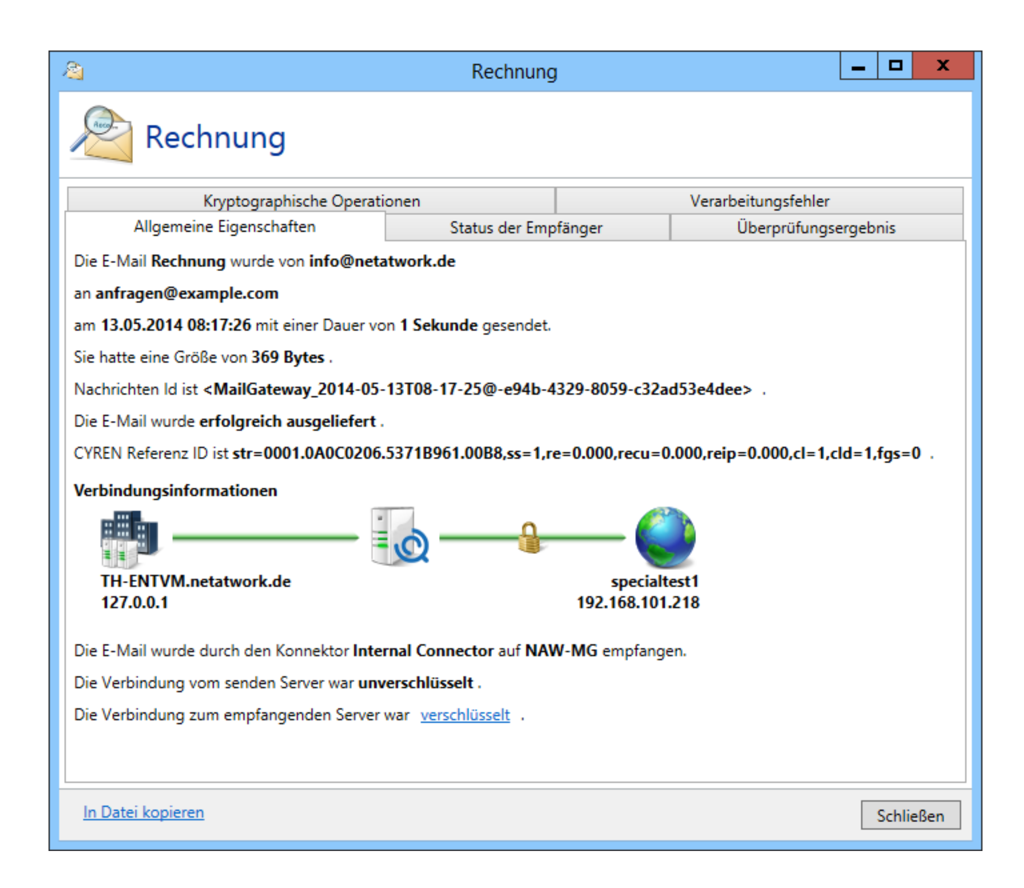


Bild 17: Das Ergebnis der E-Mail-Zustellung im Detail



Sie können die Datensätze der Nachrichtenverfolgung auch einfach auf Ihrer lokalen Festplatte abspeichern oder abgespeicherte Datensätze wieder mit allen Details anzeigen. Diese Funktion ist sehr hilfreich falls man Unterstützung bei der Analyse eines Datensatzes benötigt. Für den Export wählen Sie den Link **Nachrichtenverfolgung exportieren** in der linken unteren Ecke des Detaildialogs. Um die Details wieder anzuzeigen wählen Sie den Link **Nachrichtenverfolgungsdatei laden** in der Liste aller gefundenen Datensätze.

E-Mail-Warteschlangen

Ausgehende E-Mails werden Ihrer Domäne entsprechend in Warteschlangen gestellt. Pro Domäne gibt es eine Warteschlange. Unter dem Menüpunkt **Warteschlangenmanagement** werden Ihnen sämtliche aktiven E-Mail-Warteschlangen angezeigt (Bild 18). Hier können Sie auf einen Blick sehen, an welche Domänen noch E-Mails versendet werden müssen. Sie haben hier auch die Möglichkeit, gezielt die Übertragung an eine oder mehrere bestimmte Domänen anzuhalten.

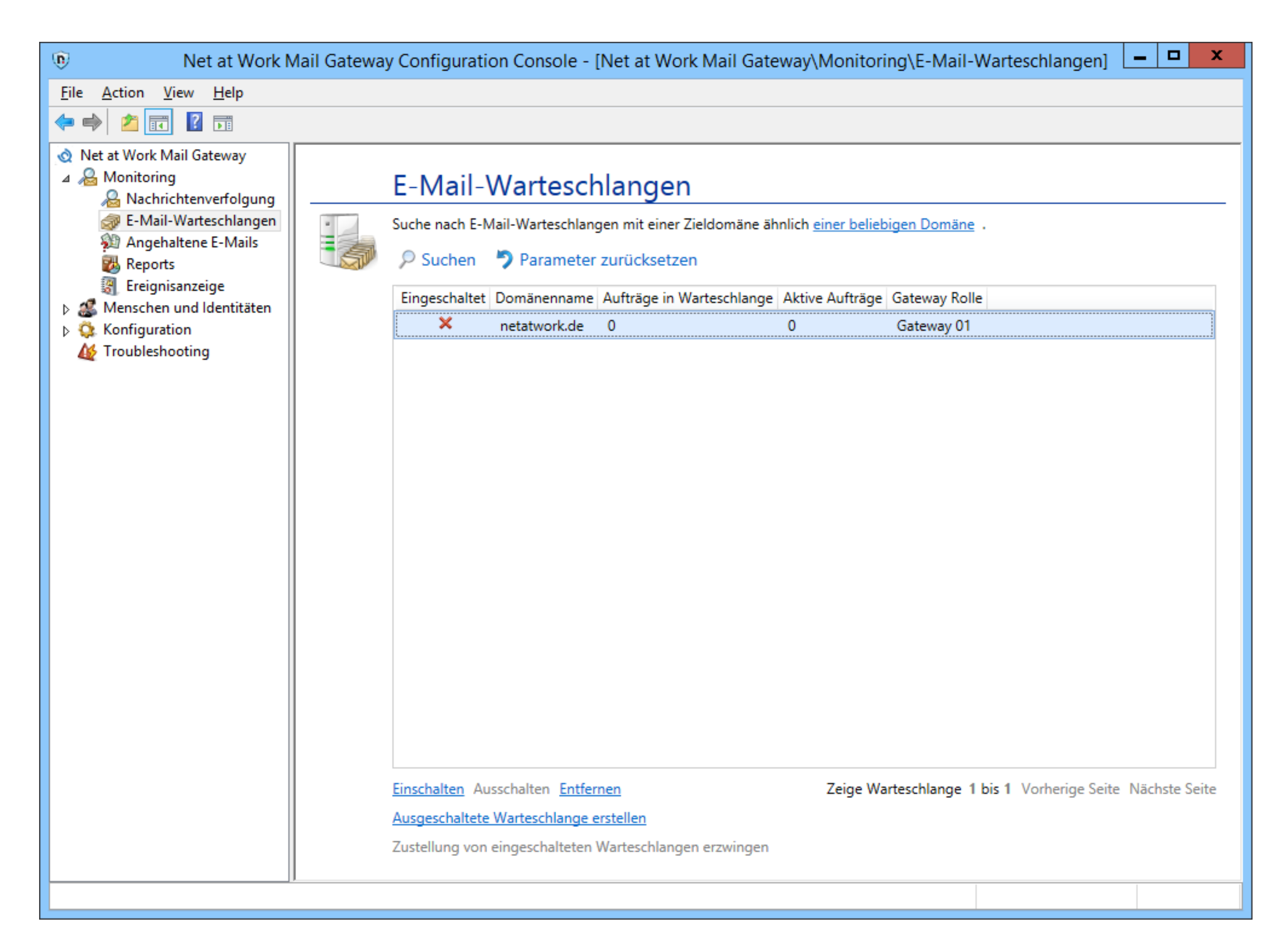


Bild 18: Alle unversandten E-Mails befinden sich, gruppiert nach Domänenname, in Warteschlangen

Mit der Suche können Sie gezielt nach Warteschlangen suchen. Geben Sie dazu den Suchbegriff in das Suchfeld ein und klicken Sie auf **Suchen**, um die Suche zu starten. Es werden Ihnen dann alle Warteschlangen angezeigt, die dem Suchbegriff entsprechen.

Die Spalte **Aktiv** ob derzeit für diese Domäne E-Mails zugestellt werden.

Der **Domänenname** entspricht dem Namen der Zieldomäne.

Die **Warteschlangenlänge** entspricht der Anzahl der wartenden E-Mails.

Die Spalte **Aktive Verbindungen** zeigt die derzeit offenen SMTP-Verbindungen zur Zieldomäne. Dies ist besonders bei einem Massenmailing interessant, in dem mehrere E-Mails an dieselbe Domäne gesendet werden.

Über die Aktion **Markierte Warteschlangen aktivieren** und **Markierte Warteschlangen deaktivieren** können Sie die Zustellung der E-Mails an die entsprechenden Domänen starten bzw. pausieren.

Sie können auch direkt eine deaktivierte Warteschlange erstellen, um die Verbindung zu einer bestimmten Domäne im Vorfeld zu unterbinden. Wählen Sie dazu **Deaktivierte Warteschlange erstellen**. Es öffnet sich der Dialog (Bild 19).

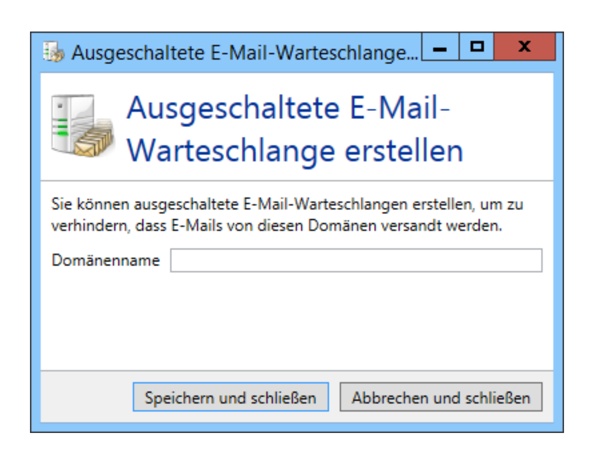


Bild 19: Domänen, zu denen keine E-Mails versandt werden sollen, können als „Deaktivierte Warteschlangen“ angelegt werden

Geben Sie unter **Domänenname für Warteschlange** den Domänennamen an (z.B. „netatwork.de“) und speichern Sie danach die Einstellung, um die deaktivierte Warteschlange zu erstellen. Es werden danach alle E-Mails an „netatwork.de“ in den Warteschlangen des Net at Work Mail Gateways pausiert, bis Sie die Warteschlange wieder aktivieren.

Eine Warteschlange kann auch gelöscht werden. Sie können beim Löschen entscheiden ob ein Nichtzustellbarkeitsbericht (NDR) gesendet wird oder nicht.

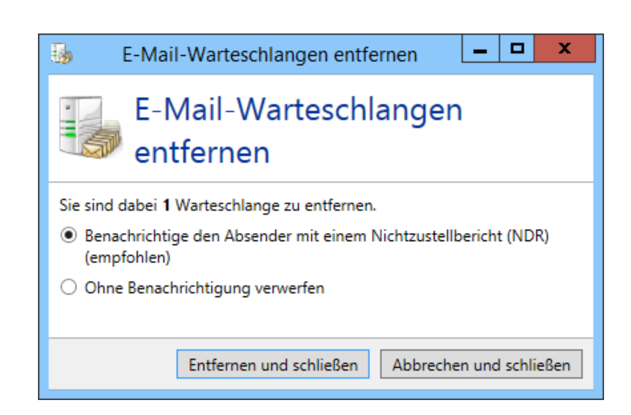


Bild 20: Entfernen von Warteschlangen

Angehaltene E-Mails

Unter bestimmten Bedingungen können E-Mails auch angehalten werden. Das bedeutet, dass bis auf weiteres die E-Mail weder zugestellt noch abgelehnt wird, sondern auf das Eintreffen bestimmter

Bedingungen wartet. Angehaltene E-Mails entstehen bei fehlenden Verschlüsselungsschlüsseln, Vorfällen durch Dateianhänge und bei Vorfällen der qualifizierten Signatur oder De-Mail. Im Knoten 'Angehaltene E-Mails' werden all diese E-Mails aufgelistet (Bild 21).

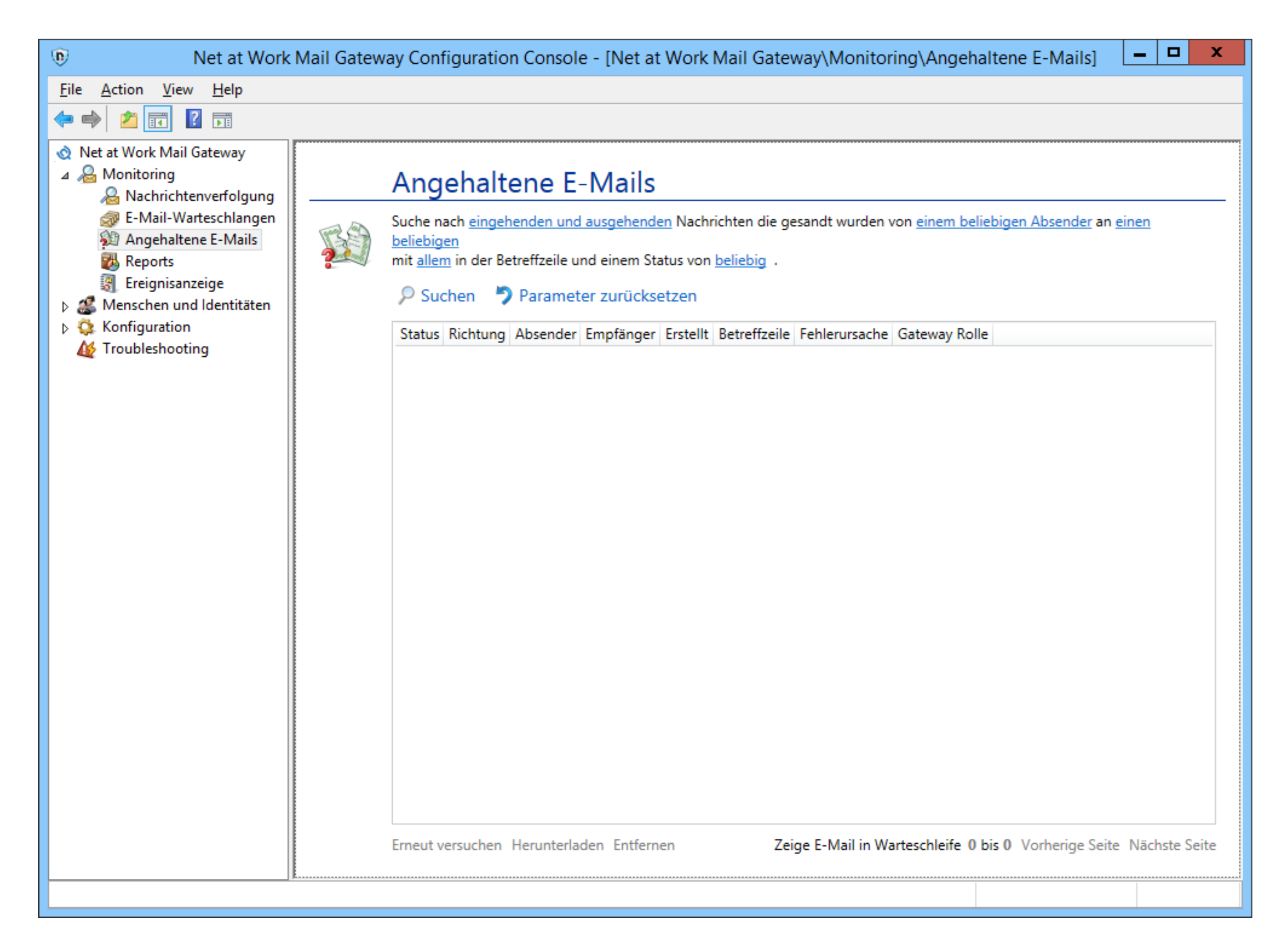


Bild 21: Die Liste aller angehaltenen E-Mails

Sie können angehaltene E-Mails suchen und filtern. Als Filter stehen Ihnen die Richtung, die Absender- und Empfängeradresse, die Betreffzeile und der Status der E-Mail zur Verfügung. Für die Adressen und Betreffzeile müssen nur Teile des zu suchenden Textes eingegeben werden. Es wird automatisch nach allen Adressen und Betreffzeilen gesucht in denen die angegebenen Teile auftauchen.

De-Mails erscheinen in der Liste falls Fehler während des Zustellprozesses auftreten.

Wenn Sie Large File Transfer lizenziert haben werden Dateien, bei denen das Hochladen in den Large File Transfer fehlschlug, hier in der Liste angezeigt.

Sie können eine erneute Verarbeitung von markierten E-Mails durch einen Klick auf **Erneut versuchen** veranlassen. Sollten erneut Vorfälle auftreten, werden die betroffenen E-Mails erneut in die Liste eingetragen.

Sie können die vollständige E-Mail mit allen zugehörigen Dokumenten auch auf dem Computer, auf dem die Benutzeroberfläche läuft, herunterladen und abspeichern. Markieren Sie dazu einen Vorfall und wählen Sie dann **Herunterladen**.



Das Löschen eines angehaltenen E-Mail löscht eine vom Net at Work Mail Gateway vollständig angenommene E-Mail. Der Absender dieser E-Mail erhält keine Benachrichtigung über diesen Vorgang und wird seinerseits von einer erfolgreichen Zustellung ausgehen.

Large files



Der Knoten ist verfügbar falls der Large File Transfer lizenziert ist.

Der Abschnitt **Dateien auf dem Web Portal** (Bild 22) zeigt alle Dateien die derzeit auf dem Web Portal gespeichert sind. Sie können an dieser Stelle Dateien löschen, die nicht mehr benötigt werden und Dateien die durch die Aktion Anhänge verwalten die Freigabe eines Administrators benötigen, auch zum herunterladen freigeben. Noch nicht freigegebene Dateien können heruntergeladen werden, um deren Inhalt zu überprüfen.

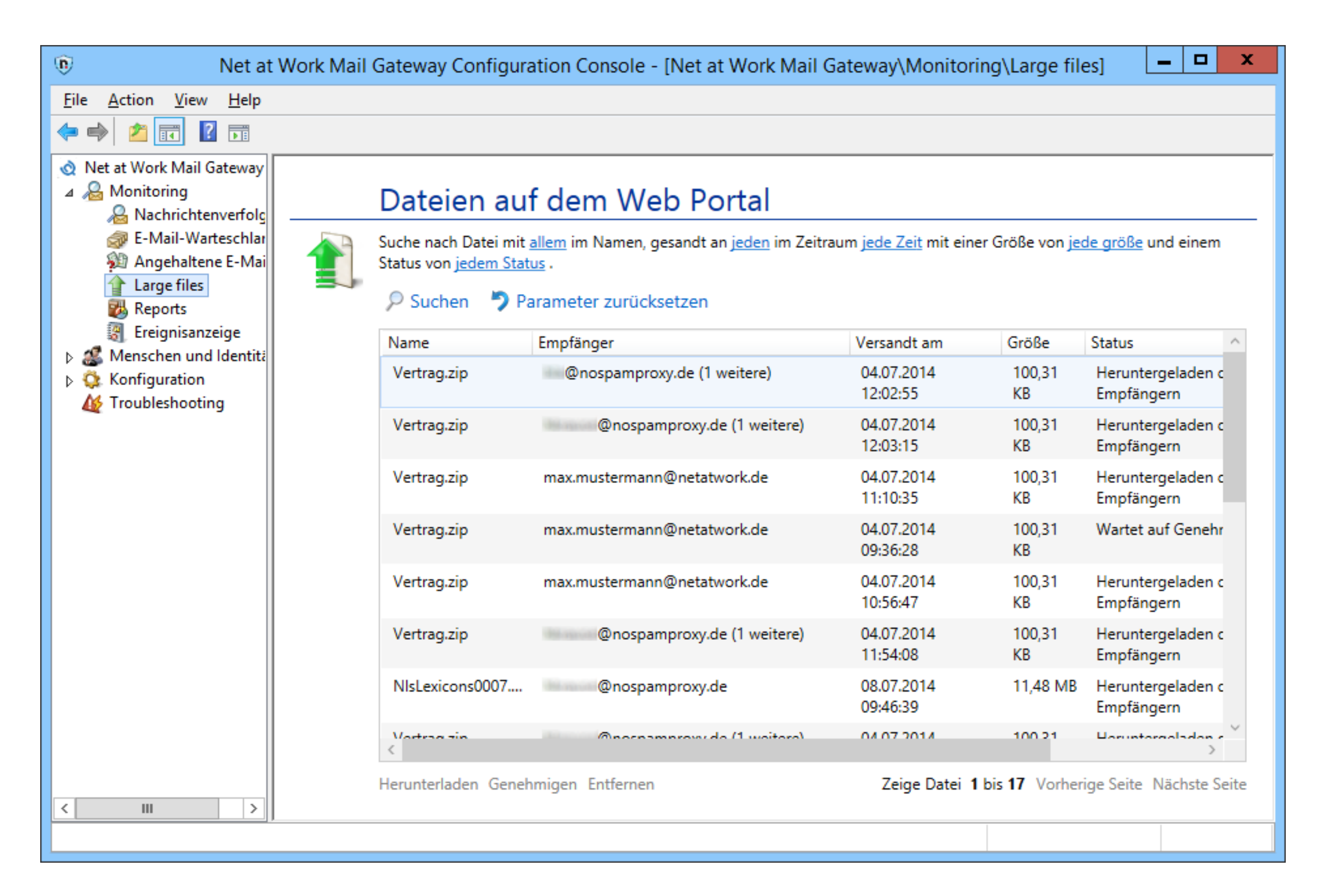


Bild 22: Die Datei auf dem Web Portal

Bei der Suche können Sie auf die folgenden Eigenschaften filtern.

- **Dateiname**
  Geben sie den Dateinamen oder Teile davon an.
- **Empfängeradresse**
  Geben Sie eine Empfängeradresse oder Teile davon an. In der Übersicht wird nur die erste Empfängeradresse angezeigt. Es kann aber nach allen Adressen gesucht werden.
- **Versandtzeitraum**
  Der Zeitraum kann eingeschräkt werden. Wenn er offen bleiben soll deaktivieren Sie die Kontrollkästchen vor **Von** und **Bis**. Durch die Auswahl unter **Zeiträume** können oft benötigte Suchen schnell gewählt werden.
- **Dateigröße**
  Schränken Sie die Dateigröße über die Schieberegler ein. Deaktivieren Sie die Einschränkung durch die Kontrollkästchen vor den Schiebereglern.
- **Status**
  Wählen Sie hier alle Dateien oder Dateien mit bestimmten Eigenschaften, wie z.B. niemals, teilweise und von allen Empfängern heruntergeladen. Es kann auch nach Dateien gesucht werden die noch nicht genehmigt wurden.

Reports

Die Reports des Net at Work Mail Gateways geben Ihnen einen Überblick über den Verlauf Ihres E-Mail-Verkehrs (Bild 23). Mit wenigen Mausklicks sehen Sie, wie sich das Spam-Aufkommen über die Monate verändert hat und welche E-Mail-Adressen bzw. Domänen das höchste Spam-Aufkommen hatten.

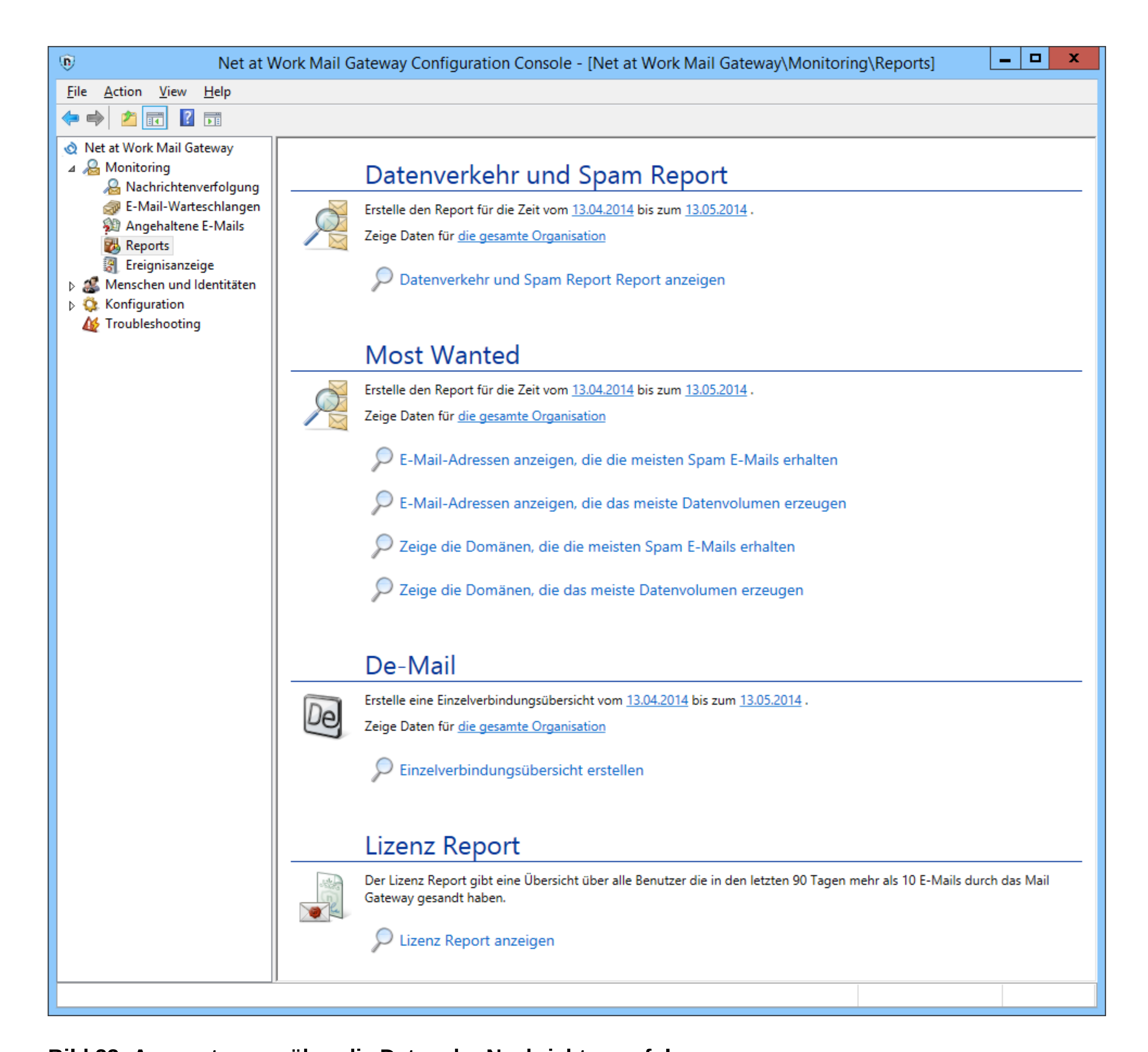


Bild 23: Auswertungen über die Daten der Nachrichtenverfolgung

Datenverkehr & Spam Report

Im Abschnitt „Datenverkehr & Spam Report“ haben Sie die Möglichkeit einen Report erstellen zu lassen, der Ihnen den Verlauf des E-Mail-Verkehrs anzeigt. Der Report zeigt sowohl den Verlauf der Anzahl der E-Mails als auch den Verlauf des Datenvolumens. Um den Report zu erstellen, wählen Sie zunächst einen Zeitraum aus, für den Sie den Report erstellen möchten. Anschließend legen Sie den Umfang des Reports fest. Klicken Sie dazu auf den Link die gesamte Organisation.

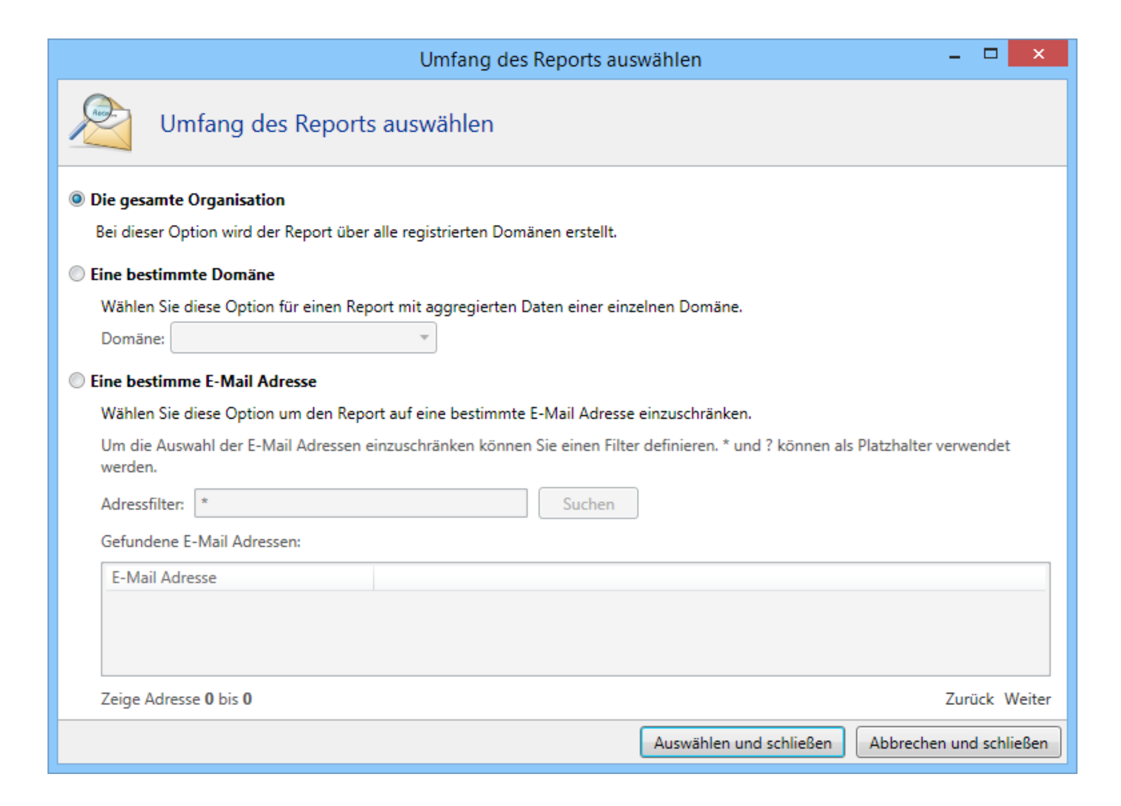


Bild 24: Der Umfang des Datenverkehr und Spam Reports

In dem erscheinenden Dialog (Bild 24) können Sie sich entscheiden, ob Sie den Report für die gesamte Organisation, nur für eine bestimmte Domäne oder sogar nur für eine bestimmte E-Mail-Adresse erstellen möchten.



Es können nur Domänen und E-Mail-Adressen ausgewählt werden, die bereits E-Mails empfangen haben und somit in der Nachrichtenverfolgungsdatenbank auftauchen. Es findet kein Zugriff auf die Konfiguration der Gateway Rolle statt.

Klicken Sie anschließend auf **Auswählen und speichern**, um die Einstellungen abzuspeichern. Anschließend klicken Sie auf **Report anzeigen**, um den Report zu erstellen.

Most wanted

Im Abschnitt **Most wanted** bietet das Net at Work Mail Gateway Ihnen vier Reports an, die zum Beispiel die E-Mail-Adressen bzw. Domänen mit dem höchsten Spam-Anteil aufweisen. Des Weiteren gibt es Reports, die Ihnen die E-Mail-Adressen bzw. Domänen anzeigen, die das meiste Datenvolumen erzeugt haben (Bild 25) Wie auch im Abschnitt **Datenverkehr & Spam Report** können Sie den Zeitraum und den Umfang des jeweiligen Reports festlegen.

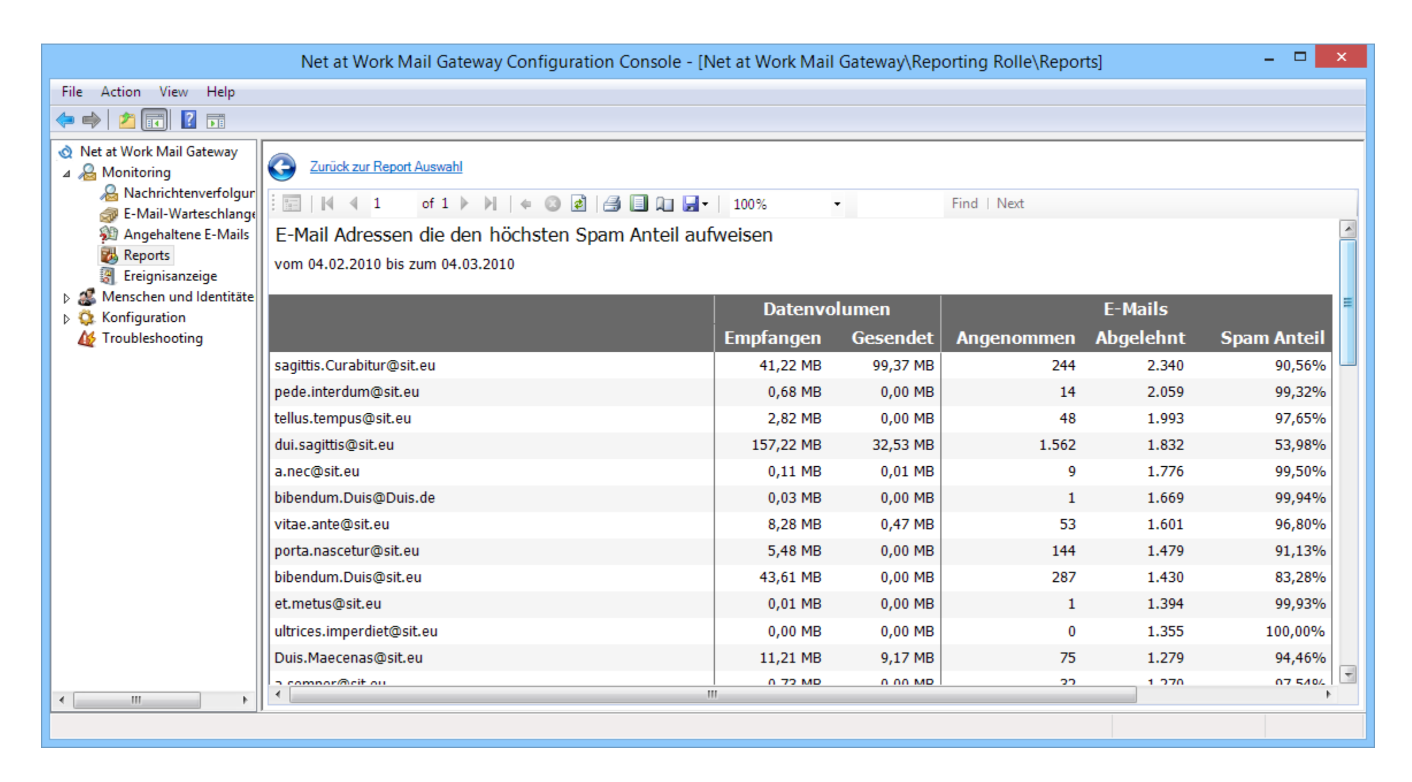


Bild 25: Die Adressen mit dem größten Spam Anteil

Die zur Verfügung stehenden Reports sind folgende:

- E-Mail-Adressen anzeigen, die die meisten Spam E-Mails erhalten.
- E-Mail-Adressen anzeigen, die das größte Datenvolumen erzeugen.
- Zeige die Domänen, die die meisten Spam E-Mails erhalten.
- Zeige die Domänen, die das größte Datenvolumen erzeugen.

Klicken Sie anschließend auf den gewünschten Report, um ihn zu generieren.

De-Mail

Mit dem De-Mail-Report können Sie eine Einzelverbindungsübersicht für gesendete De-Mails als Excel-Report erzeugen. Um den Report zu erstellen, wählen Sie zunächst aus, ob Sie eine Übersicht für die ganze Organisation oder für eine bestimmte Domäne erstellen möchten. Außerdem können Sie den

Zeitraum für die Übersicht einschränken. Klicken Sie anschließend auf **Einzelverbindungsübersicht erstellen**. Im folgenden Dialog wählen Sie aus, wo Sie die Excel-Datei speichern möchten.

Lizenz-Report

Der Lizenz-Report ist ein Hilfsmittel, die lizenzierten Benutzer der einzelnen Features, wie „NoSpamProxy" oder „enQsig", optimal auf die tatsächlich benötigten Lizenzen anzupassen (Bild 26).

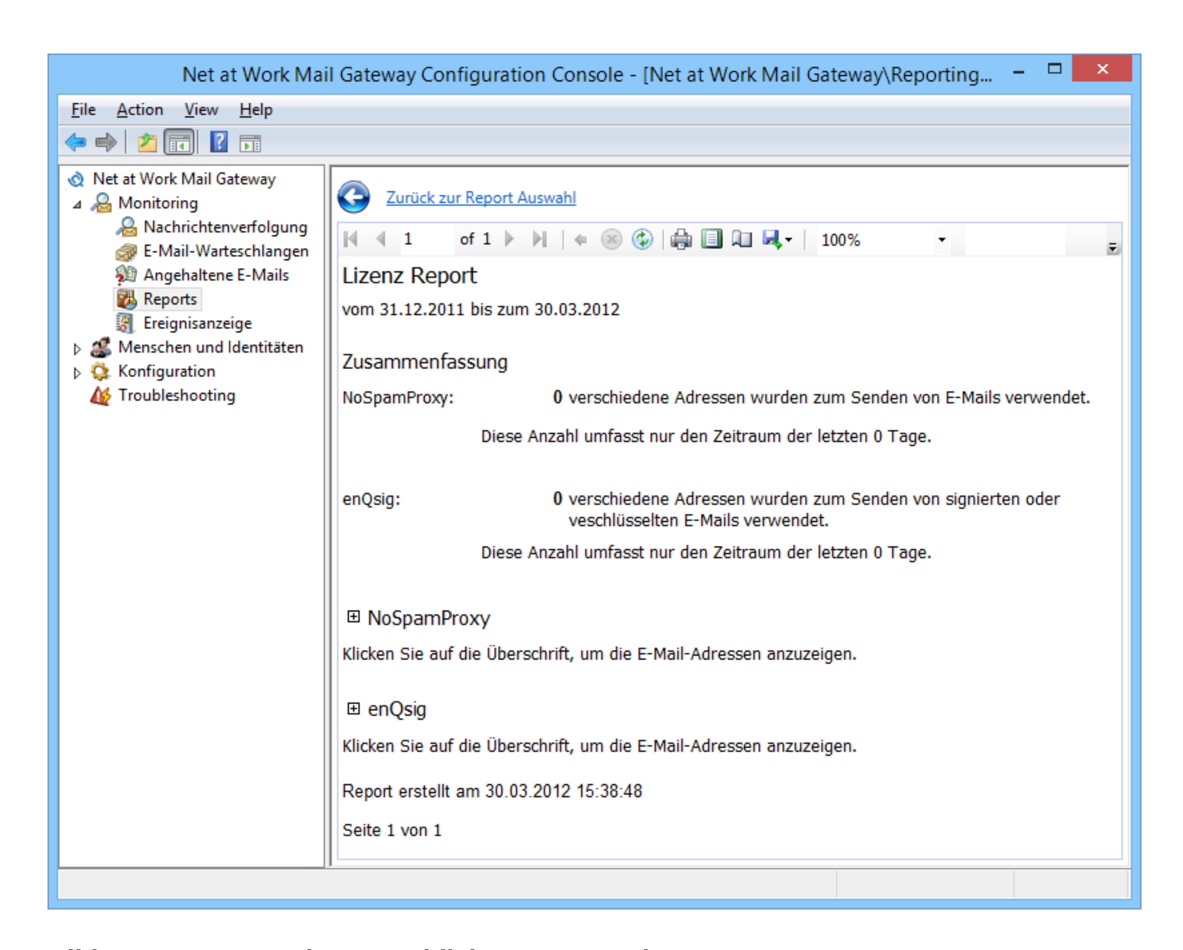


Bild 26: Der Report der tatsächlich genutzten Lizenzen

Der Lizenz-Report summiert alle Benutzer, die in den letzten 90 Tagen mehr als 10 E-Mails versandt haben. Dabei werden die verschiedenen Features „NoSpamProxy" und „enQsig" unterschieden. Für enQsig werden nur Absender von E-Mails in die Bewertung einbezogen, die signiert wurden.

Die Connector Services von enQsig CS sind nicht auf eine bestimmte Benutzerzahl beschränkt. Es gibt hier keine Einschränkungen auf bestimmte Benutzer.

Die Benutzerzahlen aus diesem Report geben Ihnen die Möglichkeit, die Lizenzen des Net at Work Mail Gateways an das Wachstum Ihres Unternehmens anzupassen.

Für Fragen zu diesem Thema steht Ihnen unser Team unter info@netatwork.de gerne zur Verfügung.

Ereignisanzeige

Die für das Net at Work Mail Gateway relevanten Server Ereignisse sind in der Oberfläche unter dem Knoten „Ereignisanzeige“ verfügbar (Bild 27).

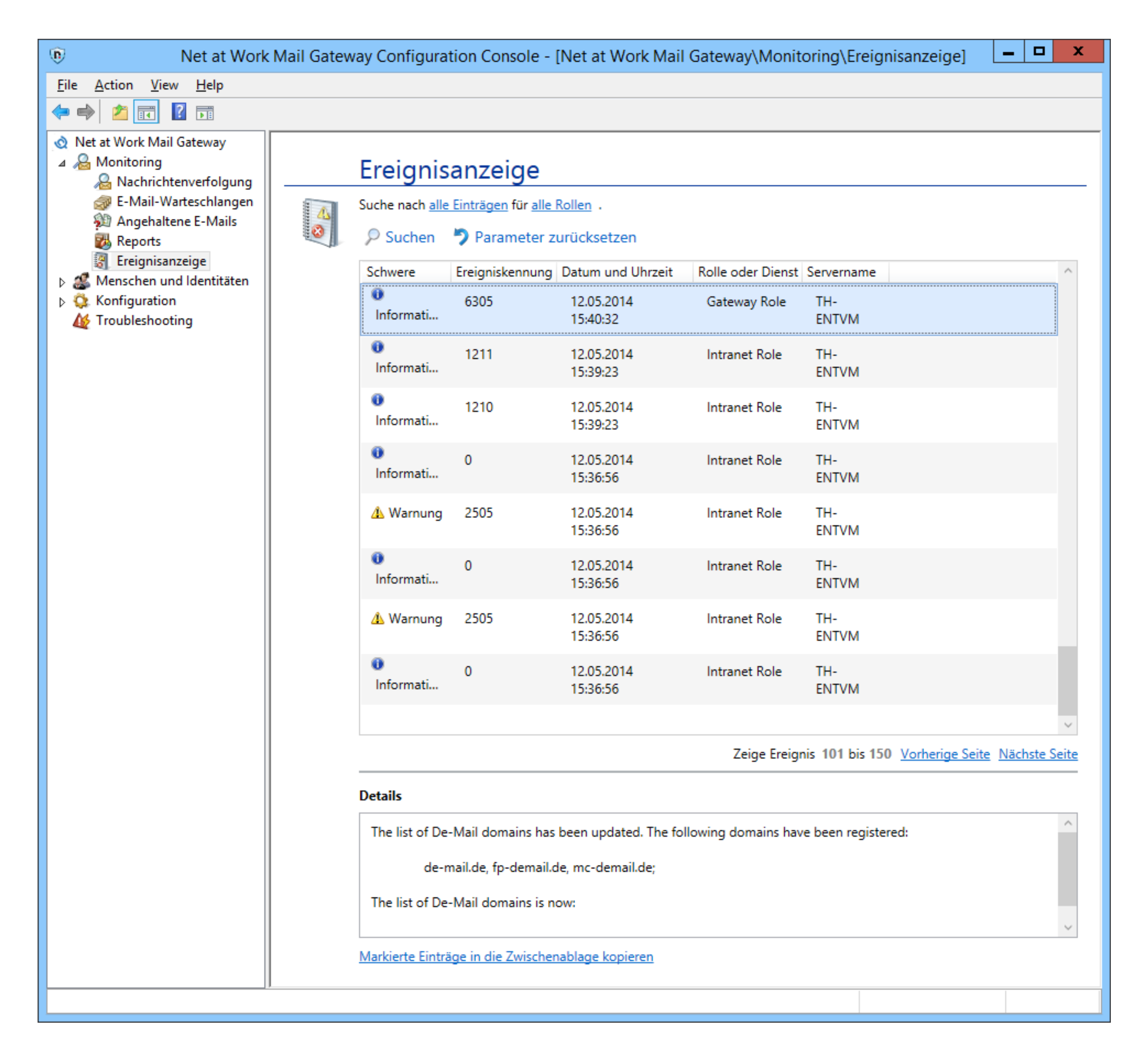


Bild 27: Die Ereignisanzeige zeigt die Ereignisse aller Rollen des Net at Work Mail Gateways an

Sie können die hier angezeigten Einträge einerseits nach den Rollen bzw. Diensten filtern, andererseits aber auch die Art der angezeigten Ereignisse einschränken. Die wählbaren Kategorien sind **Fehler**, **Informationen** und **Warnungen**. Um weiter zurückliegende Einträge anzuschauen können Sie mit den Funktionen **Zurück** und **Weiter** durch das Ergebnis der Suche blättern.

Um die Details eines Eintrags anzuzeigen, müssen Sie diesen nur mit der Maus markieren. Die Details werden im unteren Teil der Seite eingeblendet.

7. Menschen und Identitäten

Der Knoten **Menschen und Identitäten** beinhaltet alle externen und internen Firmen und Personen sowie deren E-Mail-Adressen (Bild 28).

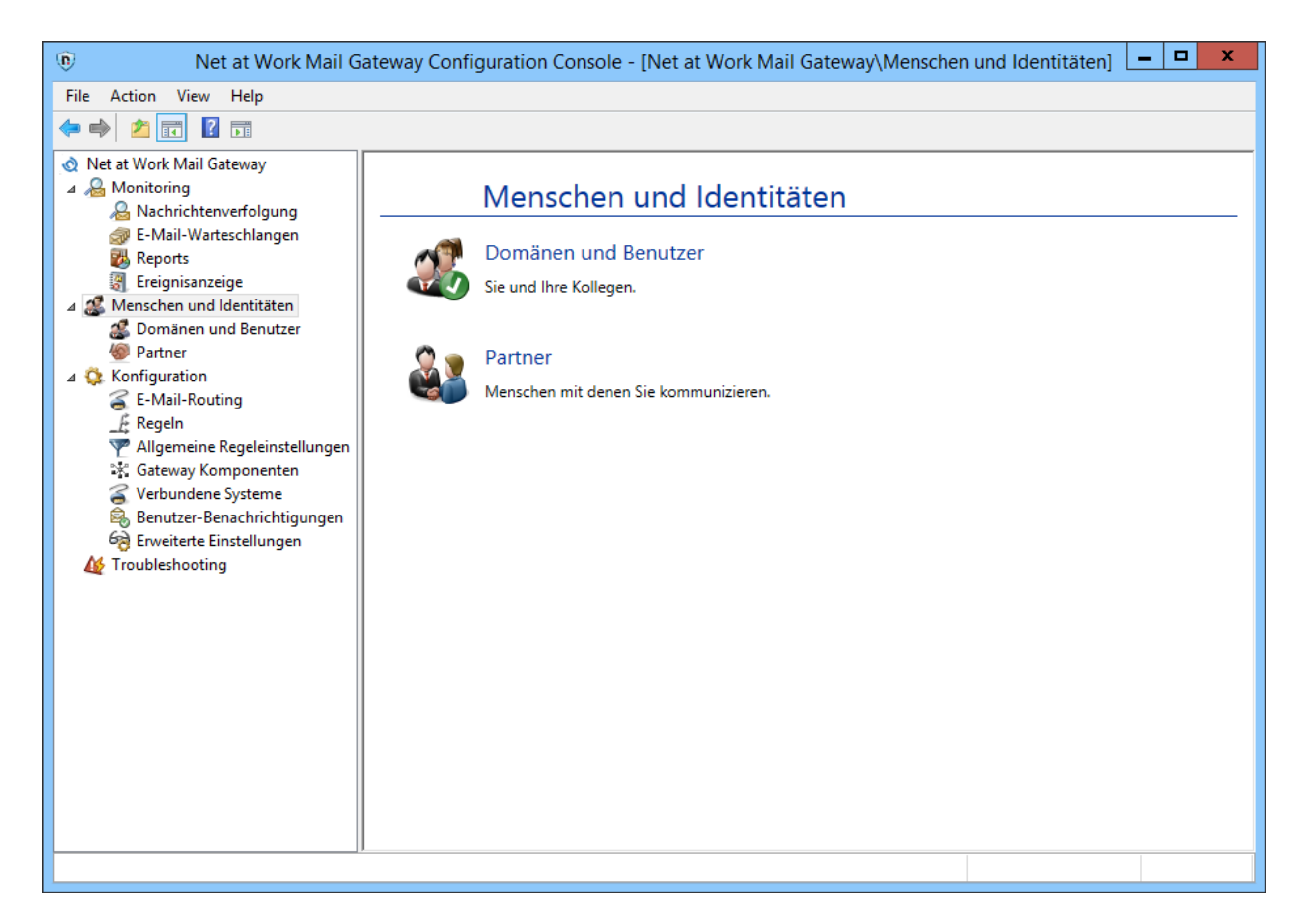


Bild 28: Die Bereiche unter dem Knoten Menschen und Identitäten

Domänen und Benutzer

Im Knoten für **Domänen und Benutzer** können Sie Ihre eigenen Domänen und eine Liste mit gültigen E-Mail-Empfängern und den zugehörigen Adressen pflegen (Bild 29). Diese Liste wird verwendet, wenn Sie in den Regeln auf „Lokale Adressen“ statt „Eigene Domänen“ filtern. Darüber hinaus können Sie hier den automatischen Import von Benutzerdaten konfigurieren.

Bild 29: Die Liste der eigenen Domänen und die lokalen Benutzer

Eigene Domänen

In die Liste der eigenen Domänen sollten Sie alle Domänen eintragen, für die Sie eingehende E-Mails empfangen wollen. Sie können diese Liste später auch in den Regeln verwenden. Andernfalls wird das Net at Work Mail Gateway solche Verbindungen als Relay-Missbrauch erkennen und diese E-Mails nicht annehmen.



Alle lokalen Domänen müssen eingetragen werden. Nur dadurch werden alle lokalen E-Mails sicher als solche erkannt und nicht als Relay-Missbrauch abgewiesen.

Eigene Domänen hinzufügen

Die Aktion **Hinzufügen** öffnet den Eingabedialog (Bild 30).

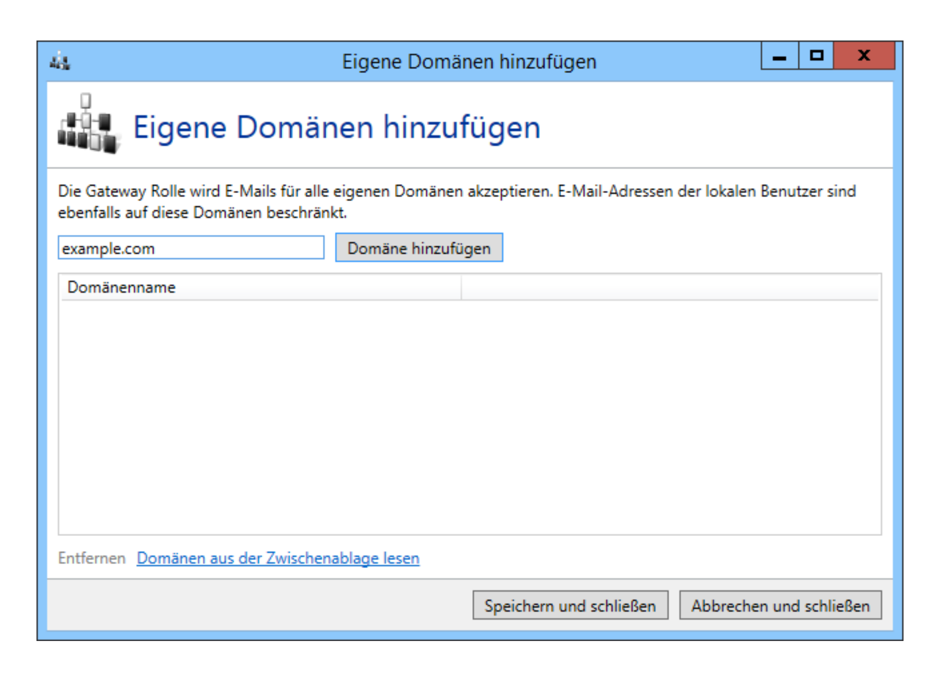


Bild 30: Dialog für neue eigene Domänen

Tragen Sie hier alle Ihre lokalen Domänen ein.



Beim Löschen von lokalen Domänen werden auch alle E-Mail-Adressen dieser Domäne aus den lokalen Benutzern gelöscht. Falls der Nutzer danach keine E-Mail-Adressen mehr besitzt wird er ebenfalls gelöscht.

Lokale Benutzer

Analog zu den "Eigenen Domänen" kann das Net at Work Mail Gateway auch die einzelnen Empfänger prüfen und E-Mails an nicht existierende Empfänger direkt abweisen. Dazu ist es aber erforderlich, dass das Gateway alle internen Empfänger kennt. Wenn Sie ein Active Directory verwenden, können Sie auf eine einfache Art und Weise die lokalen Benutzer importieren.

Die Liste der **Lokalen Benutzern** wird verwendet, wenn Sie in den Regeln auf **Lokale Adressen** statt **Eigene Domänen** filtern.



Damit das Net at Work Mail Gateway die **Lokale Benutzer** Liste auch verwendet, muss in den entsprechenden Regeln für eingehenden E-Mail-Verkehr auf der Registerkarte **Empfänger** der Radiobutton für den **Empfängertyp** von **Eigene Domänen** auf **Lokale Benutzer** gesetzt werden. Erst jetzt nutzt das Gateway die Liste der Lokalen Benutzer für die Ermittlung gültiger E-Mail-Adressen.

Die Liste der lokalen Benutzer kann zwei unterschiedliche **Typen** von Benutzern beinhalten:

- **Manuell eingetragener Benutzer**
  Sie können in manuell eingetragenen Benutzern alle Eigenschaften im Net at Work Mail Gateway verwalten. Diese Benutzer können beliebig verändert und gelöscht werden.
- **Replizierter Benutzer**
  Replizierte Benutzer werden aus einem Verzeichnisdienst wie dem Active Directory importiert. Die Eigenschaften des Benutzers müssen in der ursprünglichen Quelle verändert werden, da im Net at Work Mail Gateway bei replizierten Benutzern nur eine Lese-Ansicht der meisten Eigenschaften verfügbar ist. Alle Änderungen werden dann beim erneuten Durchlaufen der Benutzerimporte übernommen. Sie können in replizierten Benutzern sowohl den Aktivitäts-Status des kompletten Benutzers umstellen als auch den Aktivitäts-Status von einzelnen E-Mail-Adressen.

Suchen Sie nach Benutzern indem Sie nach Worten oder Wortbestandteilen im Namen, Beschreibung oder E-Mail-Adresse suchen lassen.

Benutzer hinzufügen

Wenn Sie einen neuen Benutzer hinzufügen unterstützt Sie ein Assistent. Geben Sie zuerst (Bild 31) den Namen ein. Der Name ist ein Pflichtfeld. Die optionalen Details werden für die Beantragung von Zertifikaten benötigt. Achten Sie hier auf die maximale Länge der Eingaben, der Assistent wird Sie bei der Eingabe unterstützen und alle Eingaben beim Beenden des Schrittes validieren.

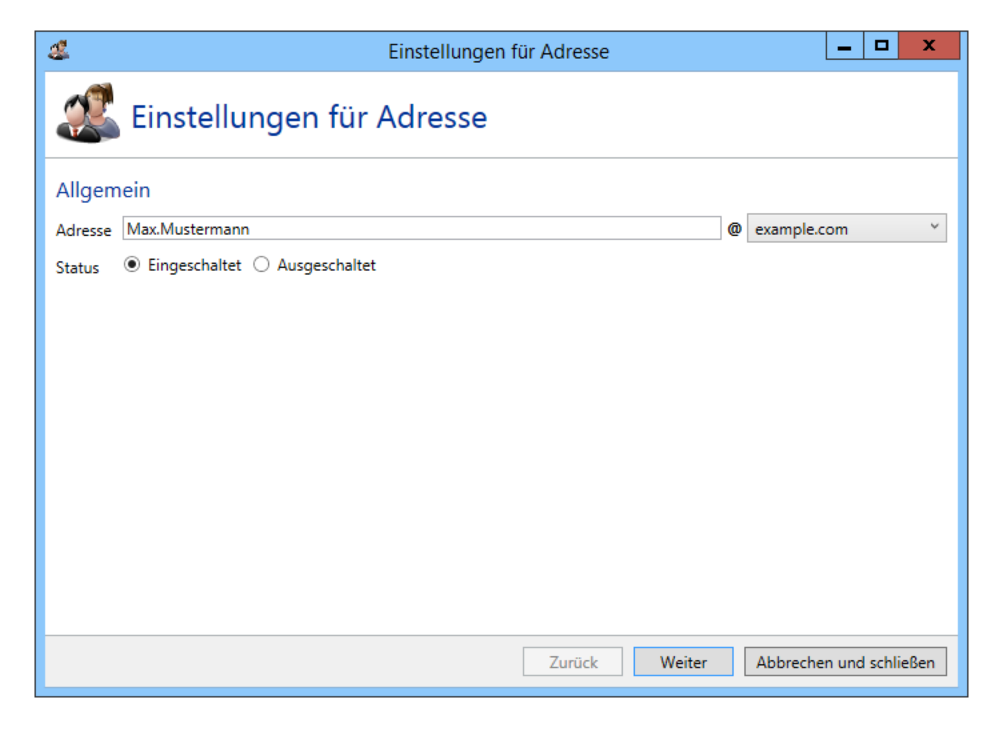


Bild 31: Der Name und die Daten des Benutzers

Im nächsten Schritt werden alle E-Mail-Adressen des Benutzers eingegeben (Bild 32).

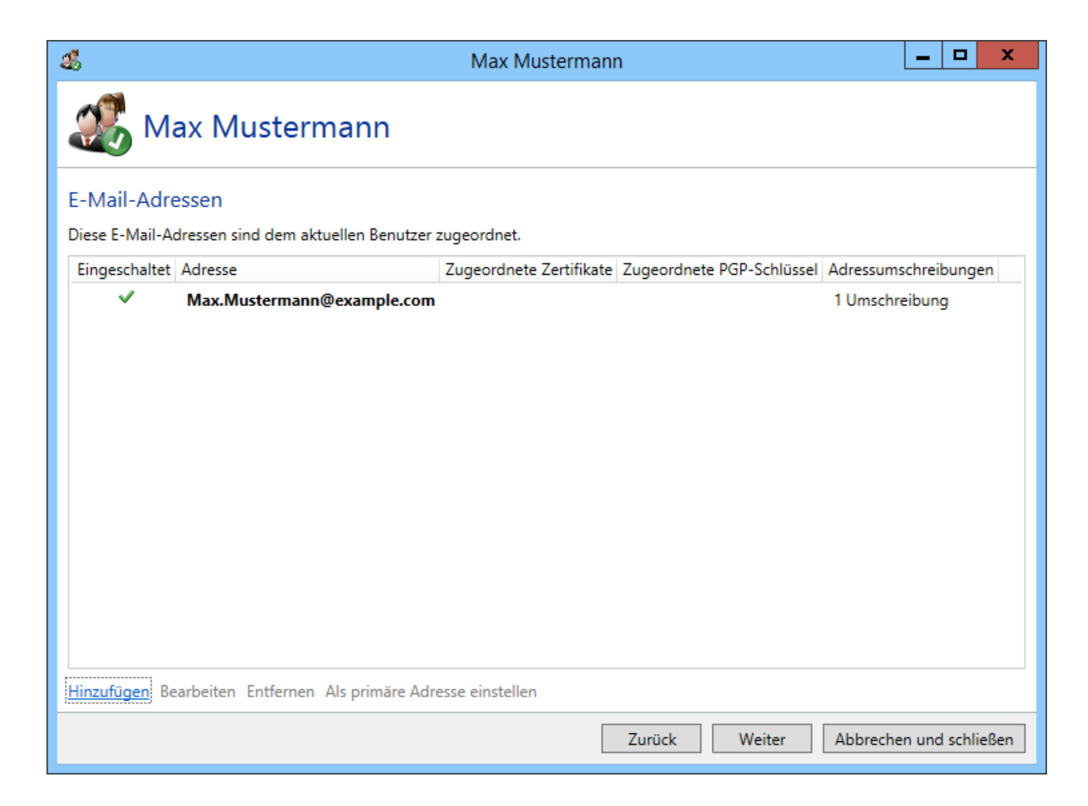


Bild 32: Alle E-Mail-Adressen die dem Benutzer zugeordnet sind

Geben Sie den lokalen Teil der E-Mail-Adresse ein und wählen Sie danach die Domäne aus der Auswahlliste Ihrer bereits eingegeben eigenen Domänen. Über **Status** kann die Adresse auch deaktiviert werden.



Die erste eingegebene Adresse wird als primäre Adresse markiert. Sie können dieses in der Liste der E-Mail-Adressen über die Aktion **Als primäre Adresse einstellen** ändern. Die primäre Adresse wird für andere Funktionen, wie z.B. De-Mail verwendet.

Der letzte Schritt (Bild 33) bestimmt alle Adressumschreibungen für diese E-Mail-Adresse.

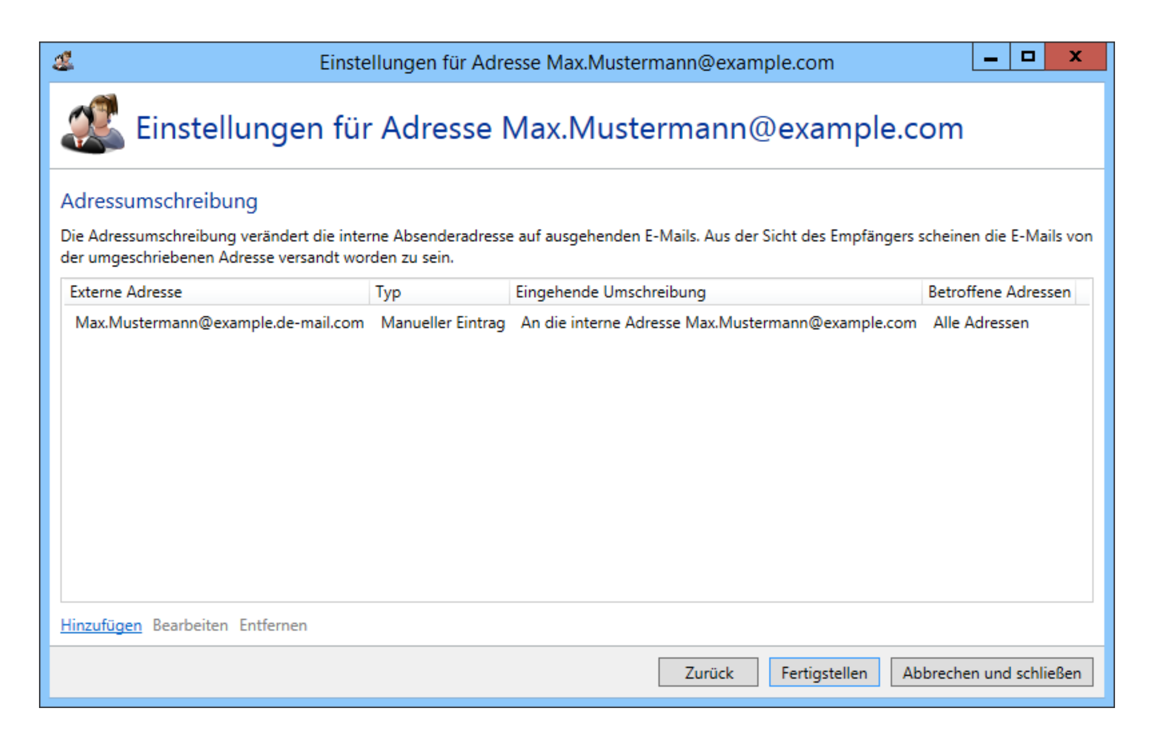


Bild 33: Die Liste aller Adressumschreibungen

Auf der Seite **De-Mail** (Bild 34) legen Sie fest, welche De-Mail-Funktionen für diesen manuell angelegten Benutzer verfügbar sind. Stellen Sie zuerst ein ob der Benutzer generell berechtigt ist De-Mails zu versenden und danach ggf. alle Bestätigungen und Auslieferungsoptionen, die dieser Benutzer anfordern kann.

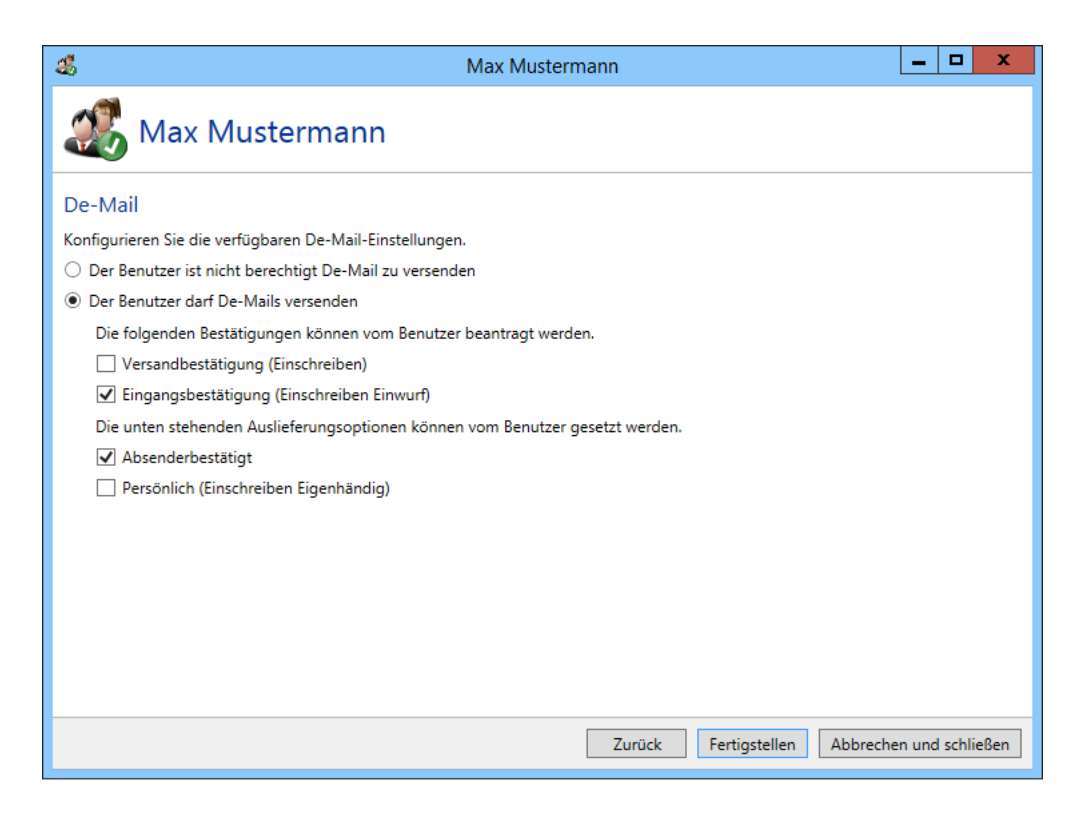


Bild 34: Verfügbare De-Mail-Funktionen für den Benutzer

Neue Adressumschreibung

Die Adressumschreibung schreibt die E-Mail-Adresse eines internen Benutzers auf eine andere E-Mail-Adresse um. Dadurch kann ein interner Nutzer gegenüber externen E-Mail-Empfängern mit einer anderen E-Mail-Adresse als seiner eigenen auftreten. Die E-Mail scheint dann von der umgeschriebenen Adresse versandt zu sein. Bei eingehenden E-Mails wird wiederum in der Liste geschaut, ob der Empfänger ein Eintrag aus den externen Adressen der Adressumschreibung ist, dann wird die Adresse an die interne Adresse des Eintrags gesandt. Ein weiterer Anwendungsfall sind sogenannte Gruppenmailboxen. In diesem Fall werden verschiedene interne E-Mail-Adressen auf eine Adresse (z.B. info@example.com) umgeschrieben.

Legen Sie bei einer Adressumschreibung zuerst die **Externe Adresse** fest die genutzt wird falls die E-Mail-Adresse umgeschrieben wird (Bild 35). Wählen Sie danach wie eingehende E-Mails behandelt werden.

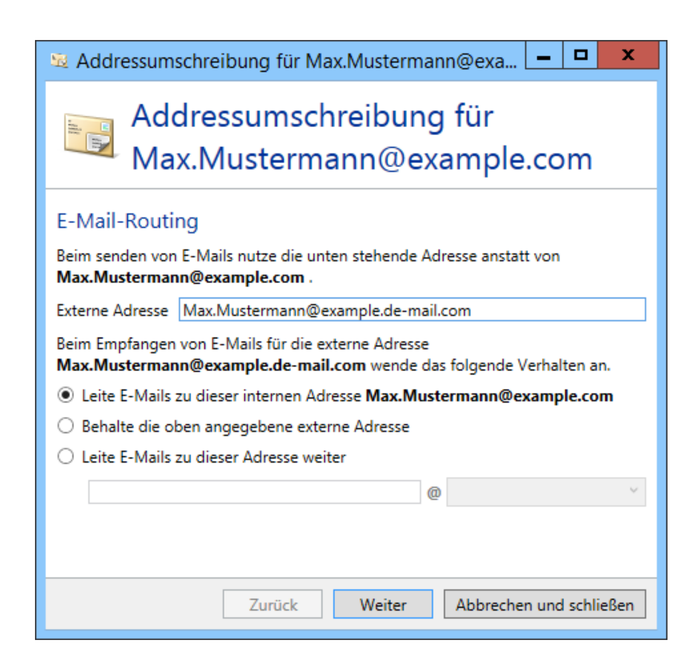


Bild 35: Externe und interne Adressen

Im nächsten Schritt wird ausgewählt bei welchen Empfängeradressen diese Umschreibung genutzt wird (Bild 36). Entspricht die Empfängeradresse nicht Ihrer Auswahl wird die Adressumschreibung nicht ausgeführt. In der Auswahl **Eine Adresse mit dem Muster** können Sie Platzhalter ('*' und '?') nutzen.

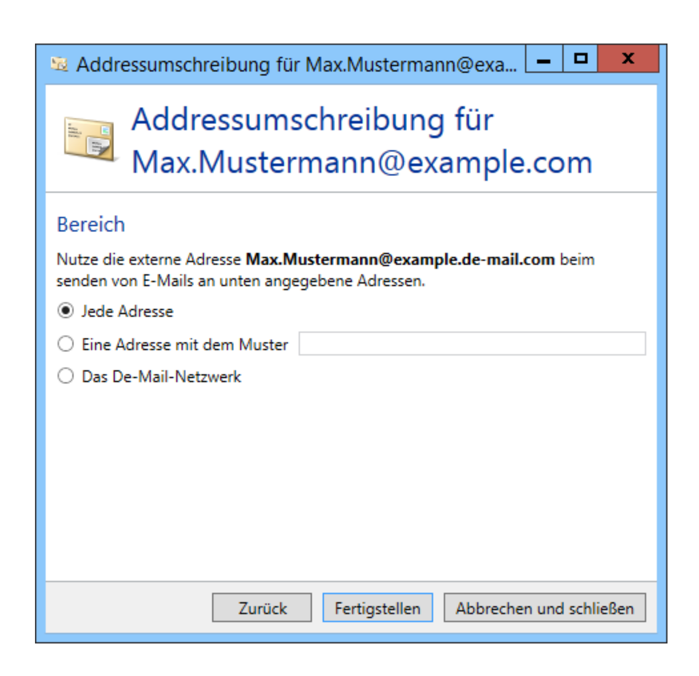


Bild 36: Gewählte Empfängeradressen dieser Umschreibung



Das Löschen von Benutzern ist für replizierte Benutzer nicht verfügbar.

Automatischer Benutzerimport

Über den Link **Automatischen Benutzerimport konfigurieren** haben Sie die Möglichkeit den Import von Benutzerdaten zu automatisieren. (Bild 37).



Bild 37: Die Liste aller eingerichteten Benutzerimporte

Sie können in der Intranet Rolle mehrere Benutzerimporte einrichten. Dies ermöglicht es Ihnen, die lokalen Benutzer in der Gateway Rolle des Net at Work Mail Gateway differenziert auf dem aktuellen Stand zu halten. So können Sie z.B. einen Import einrichten, die alle aktiven Benutzer aus dem Active Directory in die lokalen Benutzer importiert. So können Sie automatisiert sicherstellen, dass nur die von Ihnen gewünschten Adressen aus dem Internet erreichbar sind.

Neuer Benutzerimport

In einem Benutzerimport legen Sie fest, welche E-Mail-Adressen importiert werden sollen. Als Quelle können Sie entweder ein Active Directory oder eine Textdatei angeben. Des Weiteren legen Sie fest, wann oder in welchen zeitlichen Abständen ein Durchlauf stattfinden soll.

Beim Hinzufügen eines neuen Benutzerimports legen Sie im ersten Schritt den Typ fest. (Bild 38). Sie können aus dem Active Directory, einer generischen LDAP-Quelle, wie zum Beispiel Lotus Notes, oder einer Textdatei importieren.

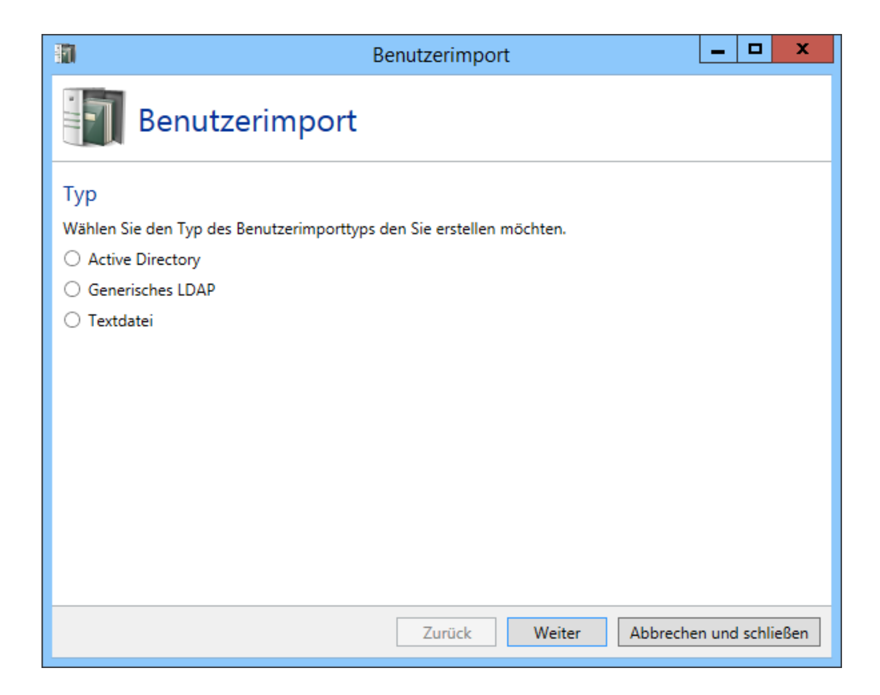


Bild 38: Typ des Benutzerimports

Im Schritt **Allgemein** (Bild 39) geben Sie einen eindeutigen Namen für den Benutzerimport an. Legen Sie dann unter **Aktualisierungszyklus** fest wenn der Benutzerimport durchgeführt wird. Über **Status** können Sie den Import auch abschalten ohne ihn zu löschen.

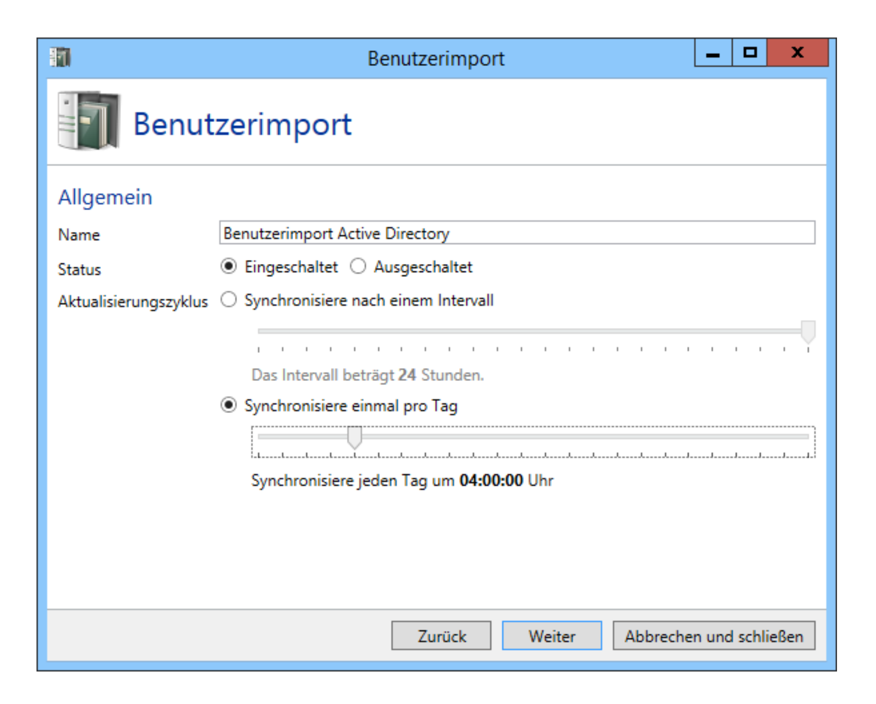


Bild 39: Allgemeine Einstellungen

Lesen Sie jetzt bitte, je nach ausgewähltem Typ, in dem Kapitel Active Directory, Generisches LDAP oder Textdatei.

Active Directory

In der **Active-Directory-Verbindung** stellen Sie die Verbindung mit Ihrem Domänenkontroller her (Bild 40). Wählen Sie dazu die Art des Servers und den Benutzer, der darauf zugreifen darf. Wenn Sie einen bestimmten Domänenkontroller eintragen möchten, können Sie eine IP-Adresse oder einen Servernamen eintragen. Bei Auswahl der integrierten Windows Authentifizierung nutzt das Mail Gateway den Netzwerkdienst, falls es auf einem Domänenkontroller installiert wurde, ansonsten wird das Computerkonto zur Authentifizierung verwendet.

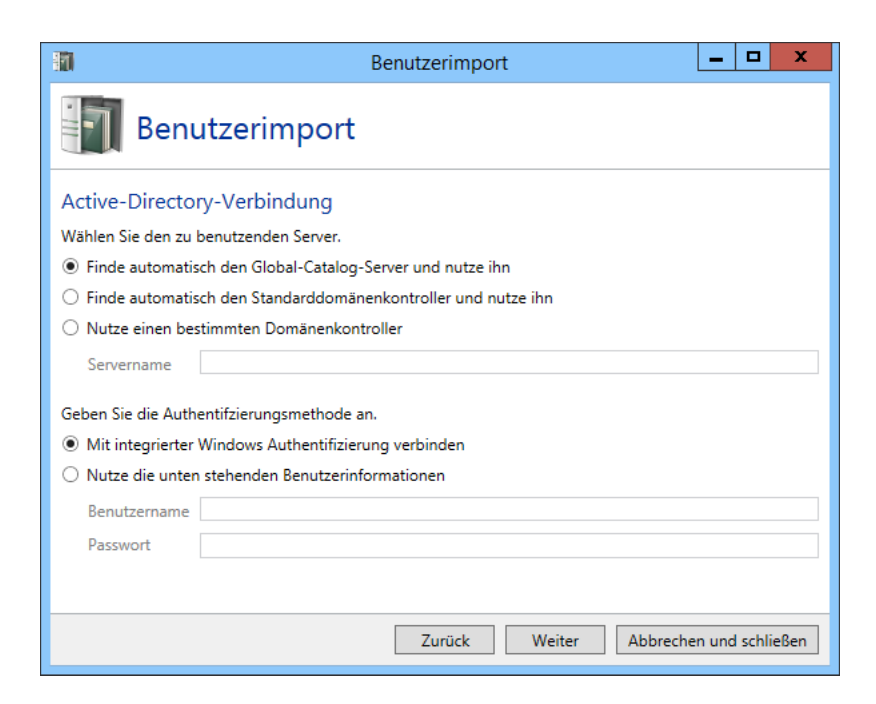


Bild 40: Die Verzeichnisverbindung

Die **Active-Directory-Suche** wählt die Benutzer aus, die importiert werden. Sie können hier auf bestimmte Container filtern, z.B.:

`OU=Vertrieb,OU=User,DC=domäne,DC=DE`.

Ersetzen Sie bei der Benutzung des Beispiels „Vertrieb“, „User“, „domäne“ und „DE“ mit passenden Werten.

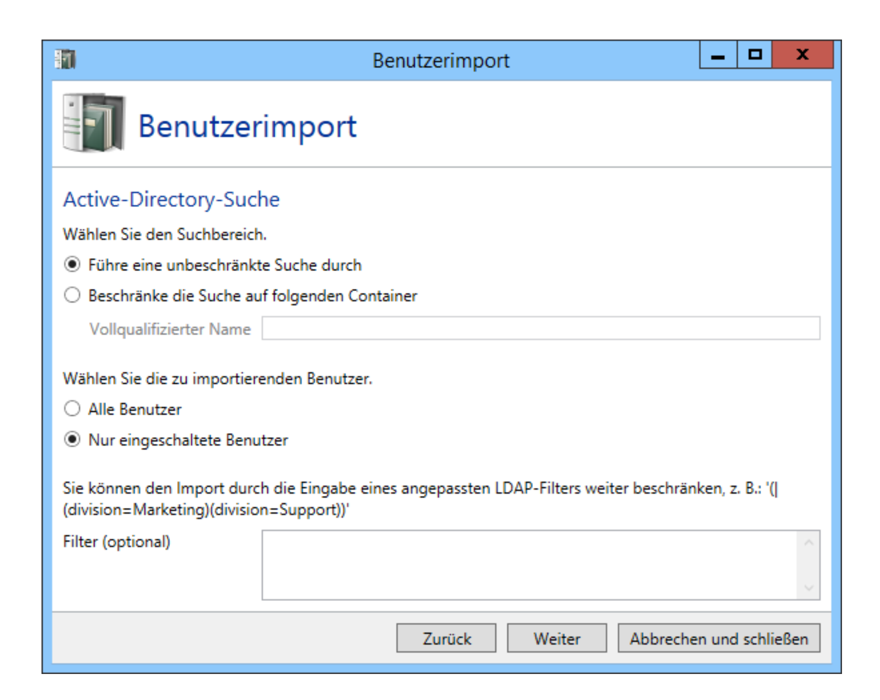


Bild 41: Die Auswahl der zu importierenden Active Directory Benutzer

Sie können auch die Art der zu importierenden Benutzer auswählen sowie zusätzliche LDAP-Filter angeben. Damit Sie zum Beispiel nur Benutzer importieren, die ein bestimmtes Attribut mit einem bestimmten Wert gefüllt haben.

In den **Gruppen** (Bild 42) geben Sie an welche Funktionen des Mail Gateway jeder lokale Nutzer, der importiert wurde, nutzen darf. Die Funktionen sind dabei abhängig von seiner Gruppenmitgliedschaft.



Bild 42: Berechtigte Gruppen für De-Mail

Generisches LDAP

Die **LDAP-Verbindung** (Bild 43) baut die Verbindung zu Ihrem Server auf. Geben Sie den Server und die zu benutzenden Anmeldeinformationen ein.

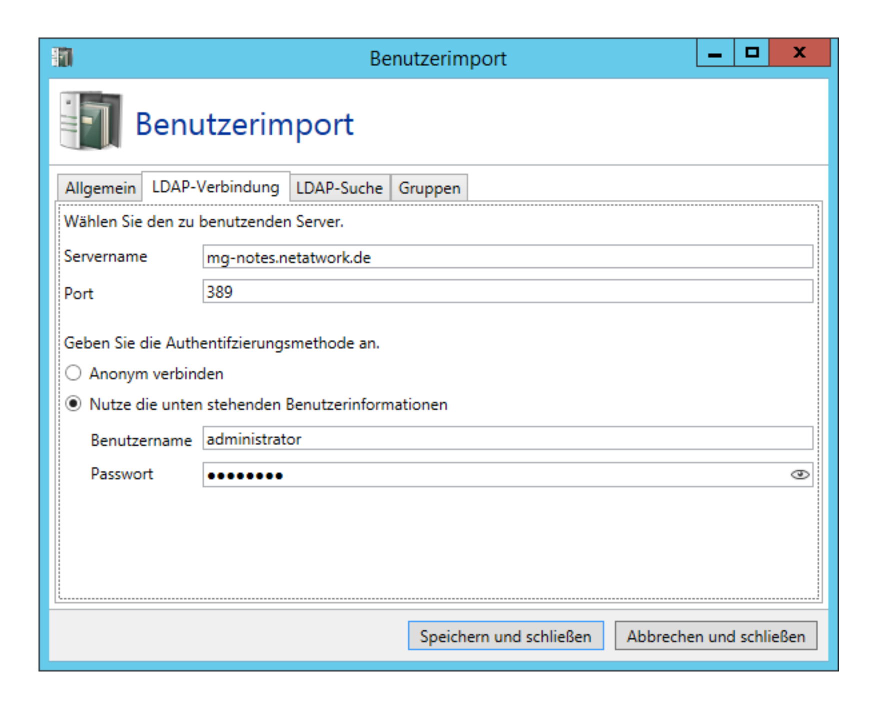


Bild 43: Berechtigte Gruppen für De-Mail

In der **LDAP-Suche** (Bild 44) könne Sie die Suche im Verzeichnis auf bestimmte Container einschränken. Geben Sie bitte Klassennamen an unter dem die Gruppen zu finden sind. Zusätzlich können Sie mit einem Filter die Suche auf Benutzer mit bestimmten Eigenschaften beschränken.

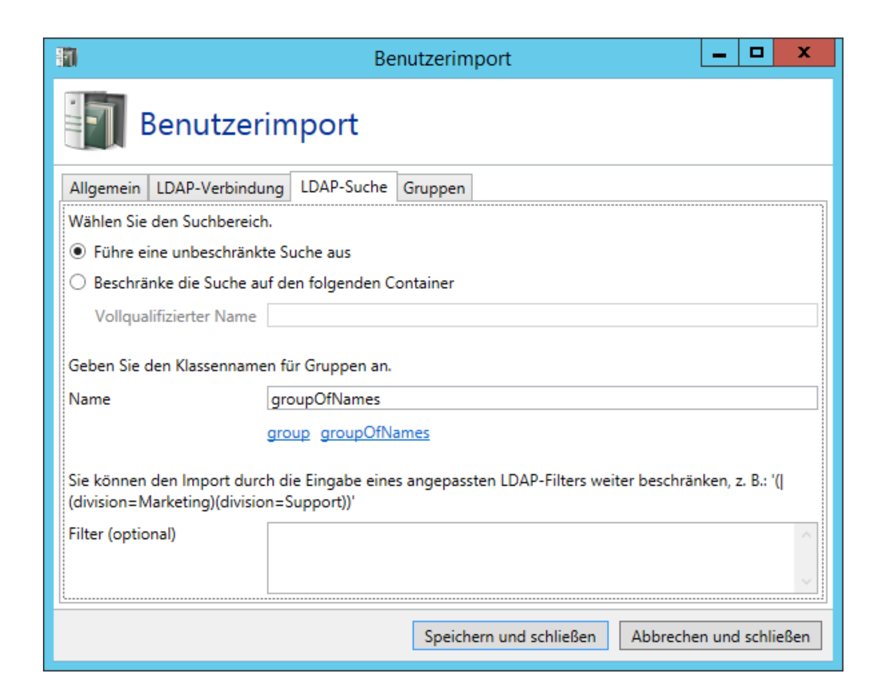


Bild 44: Berechtigte Gruppen für De-Mail

In den **Gruppen** (Bild 45) geben Sie an welche Funktionen des Mail Gateway jeder lokale Nutzer, der importiert wurde, nutzen darf. Die Funktionen sind dabei abhängig von seiner Gruppenmitgliedschaft.

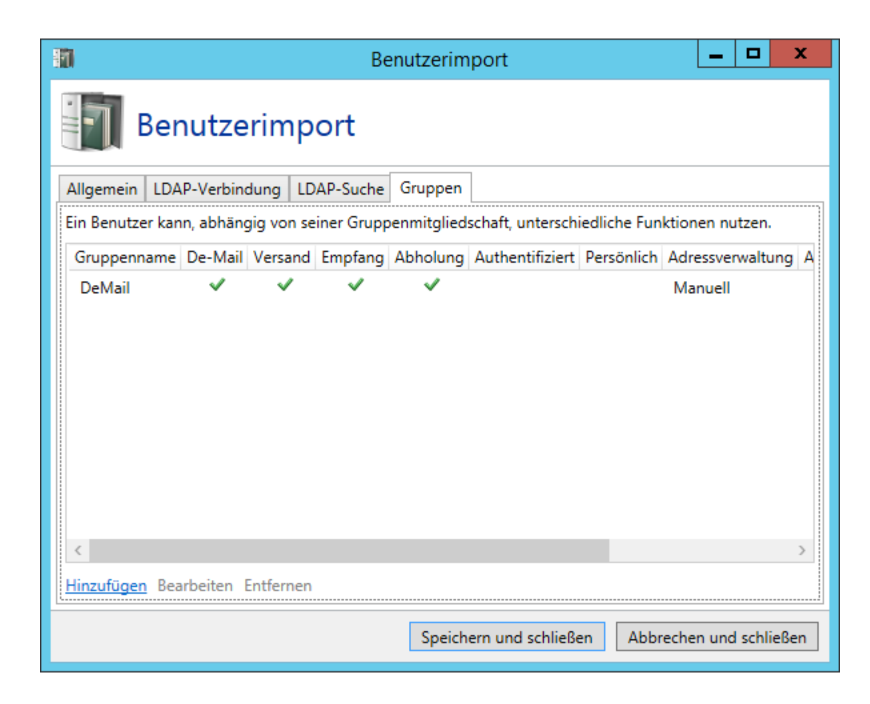


Bild 45: Berechtigte Gruppen für De-Mail

Textdatei

In den Einstellungen für den Benutzerimport durch Textdateien geben Sie bitte den Pfad zu der Datei mit den Benutzeradressen an (Bild 46).



Bild 46: Die Angabe des Pfads zur Textdatei



Die Text-Datei benötigt kein spezielles Format. Es werden alle E-Mail-Adressen, in einem beliebig formatierten Text, gefunden und importiert.

Neue Gruppe im Benutzerimport

Um Funktionen des Mail Gateways für Benutzergruppen freizugeben muss die Active-Directory-Verbindung oder die LDAP-Verbindung konfiguriert sein. Suchen Sie nach der Gruppe, die Sie berechtigen wollen und wählen Sie diese dann aus (Bild 47).

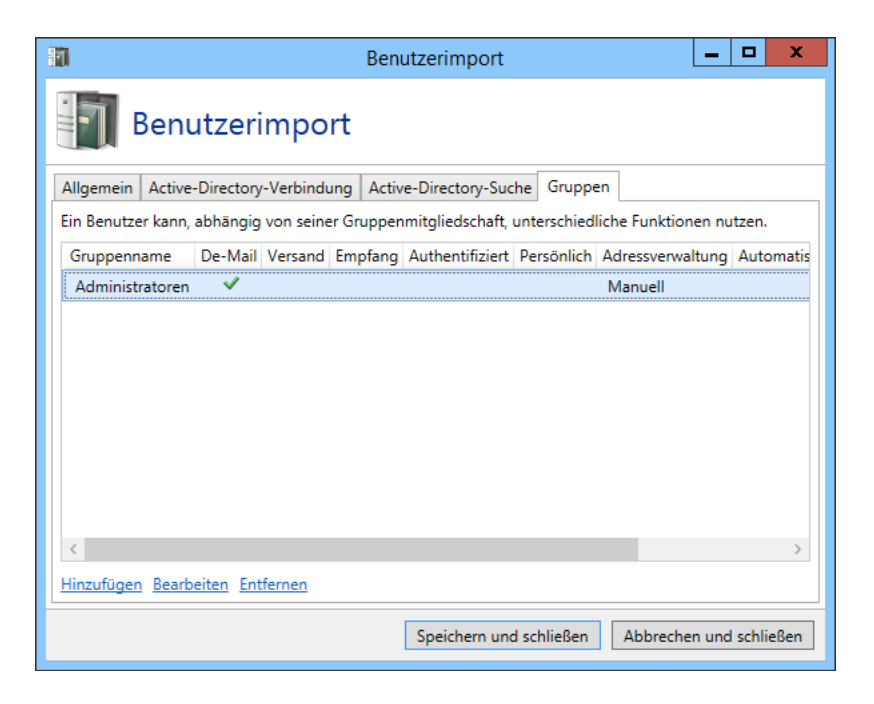


Bild 47: Die Auswahl der Benutzergruppen

In den De-Mail Berechtigungen (Bild 48) legen Sie fest welche De-Mail Funktionen den Mitgliedern dieser Gruppe zu Verfügung gestellt werden.

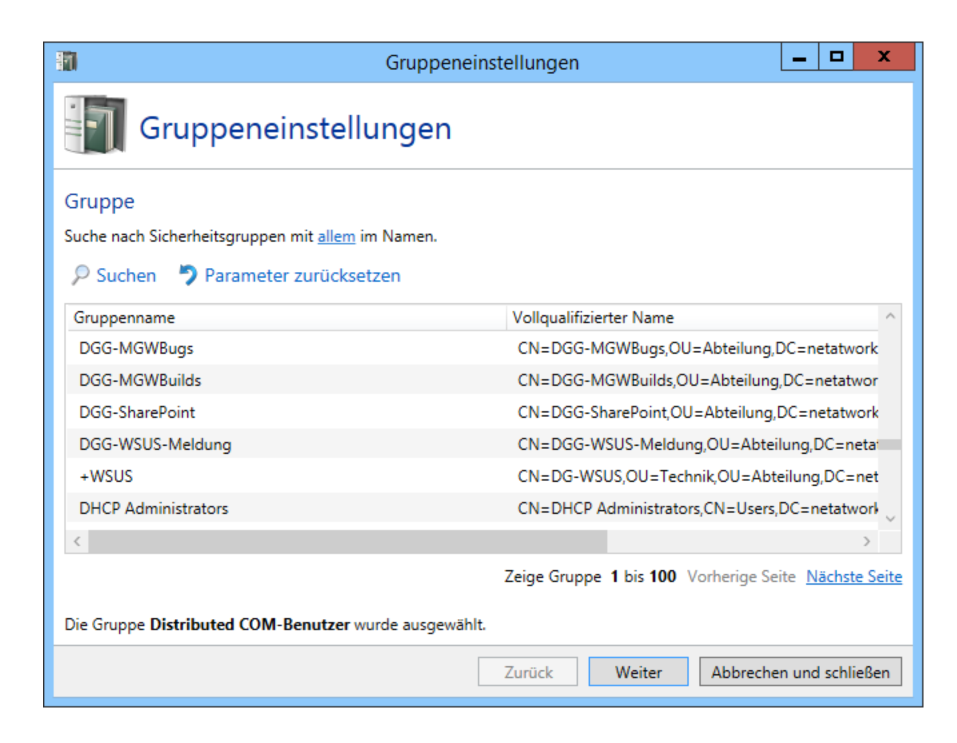


Bild 48: Berechtigungen der gewählten Gruppe auf De-Mail-Funktionen

Jeder Benutzer, der De-Mail nutzen will benötigt eine De-Mail-Adresse. Diese können Sie über die **Adressverwaltung** (Bild 49) nach einem Ersetzungsmuster erstellen lassen oder auch manuell über den Knoten Adressumschreibung. Sollten Benutzer keine gültige De-Mail-Adresse besitzen wird für diese im Ereignisprotokoll eine Warnung angezeigt.



Ist es den Mitgliedern der Gruppe nicht erlaubt De-Mails zu versenden, dann ist dieser Dialog nicht benutzbar.

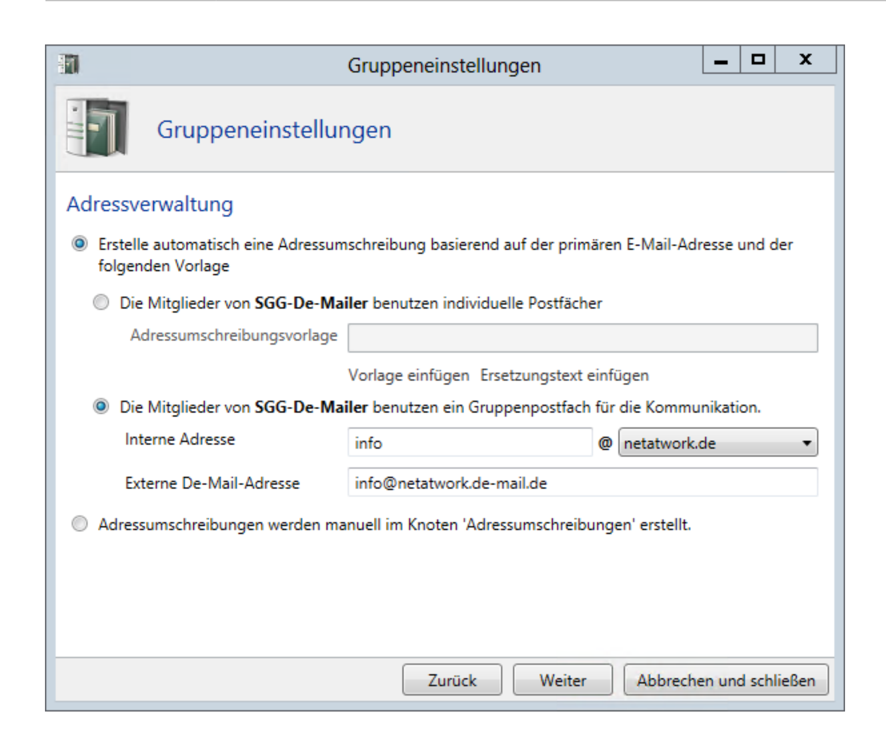


Bild 49: Die Verwaltung der De-Mail-Adressumschreibungen

Wählen Sie zunächst aus, ob die Adressumschreibung automatisch nach dem hinterlegten Muster oder manuell über den Adressumschreibungsknoten erstellt werden soll. Möchten Sie die Adressumschreibungen automatisch erstellen lassen, können Sie entweder individuelle Einträge erstellen lassen oder die Gruppen-Mailbox-Funktionalität nutzen. Bei individuellen Einträgen wird für jeden Benutzer für dessen primäre E-Mail-Adresse eine eindeutige De-Mail-Adresse generiert. Hierfür hinterlegen Sie in dem Dialog eine Vorlage, nach der die Adresse erstellt werden soll. Es stehen Ihnen die folgenden Ersetzungseinträge zur Verfügung.

- **Vorname %g**
  Bei der Benutzung von '%g' wird der Vorname des Benutzers eingesetzt. Beispielsweise wird für den Benutzer 'Eva Musterfrau' der Vorname 'Eva' eingefügt.
- **Erster Buchstabe des Vornamen %1g**
  Bei der Benutzung von '%1g' wird der erste Buchstabe des Vornamens des Benutzers eingesetzt. Sie können statt '1' auch andere Zahlen einsetzen um mehrere Buchstaben des Nachnamen zu

benutzen. Beispielsweise wird für den Benutzer 'Eva Musterfrau' bei Benutzung von '%2g' der Teil 'Ev' des Vornamen eingefügt.

- **Nachname %s**
  Bei der Benutzung von '%s' wird Nachname des Benutzers eingesetzt. Beispielsweise wird für den Benutzer 'Eva Musterfrau' der Nachname 'Musterfrau' eingefügt.
- **Erster Buchstabe des Nachnamen %1s**
  Bei der Benutzung von '%1s' wird der erste Buchstabe des Nachnamens des Benutzers eingesetzt. Sie können statt '1' auch andere Zahlen einsetzen um mehrere Buchstaben des Nachnamen zu benutzen. Beispielsweise wird für den Benutzer 'Eva Musterfrau' bei Benutzung von '%7s' der Teil 'Musterf' des Nachnamen eingefügt.
- **Lokaler Teil %p**
  Bei der Benutzung von '%p' wird der lokale Teil der primären E-Mail-Adresse eingesetzt. Beispielsweise wird für die Adresse 'max.mustermann@example.com' der lokale Teil 'max.mustermann' eingefügt.
- **Domäne ohne TLD %c**
  Bei der Benutzung von '%c' wird die Domäne der primären E-Mail-Adresse ohne die Top-Level-Domain wie '.de', '.net', '.com' usw. eingesetzt. Beispielsweise wird für die Domäne 'example.com' der Domänenname 'example' eingefügt.

Nutzen Sie eine der vordefinierten Ersetzungsvorlagen und passen Sie sie ggf. an falls Sie den Ersetzungseintrag nicht vollständig manuell erstellen möchten. Alternativ kann die Gruppen-Mailbox-Funktionalität verwendet werden. In diesem Fall verwenden alle Mitglieder der Gruppe dieselbe De-Mail-Adresse. Eingehende De-Mails werden dann an eine bestimmte interne E-Mail-Adresse geleitet.



Es werden nur E-Mail-Adressen importiert, wenn die Domäne auch in den Eigenen Domänen des Net at Work Mail Gateways hinterlegt ist. Alle anderen werden nicht importiert.

Partner

Ein Partner definiert die Sicherheits- und bei lizenziertem NoSpamProxy auch die Vertrauenseinstellungen zu einer externen Domäne oder E-Mail-Adresse. Die Sicherheitseinstellungen einer Domäne oder E-Mail-Adresse umfassen die folgenden Punkte.

- **Notwendige Transportsicherheit**
  Sie können bestimmen, dass E-Mails während des Transports von Server zu Server verschlüsselt werden müssen. Sie können zusätzlich auch Anforderungen an das verwendete Zertifikat stellen und zusätzliche erlaubte Zertifikate hinterlegen. Die notwendige Transportsicherheit wird immer für die gesamte Domäne festgelegt.
- **Vertrauen**
  Das Mail Gateway gibt Ihnen außerdem die Möglichkeit zu definieren, wie stark Sie dieser Domäne vertrauen. Vertrauen wird automatisch durch die laufende E-Mail-Kommunikation mit einem Partner aufgebaut. Sie können diese Einstellungen in dem Domäneneintrag beeinflussen.

In der Übersicht werden alle angelegten Partnerdomänen angezeigt (Bild 50). Neben der Domäne werden in jeder Zeile die zusätzlich angelegten E-Mail-Adressen in der Spalte **Benutzereinträge** aufgeführt sowie die Einstellungen zum **Vertrauen** in den Partner.

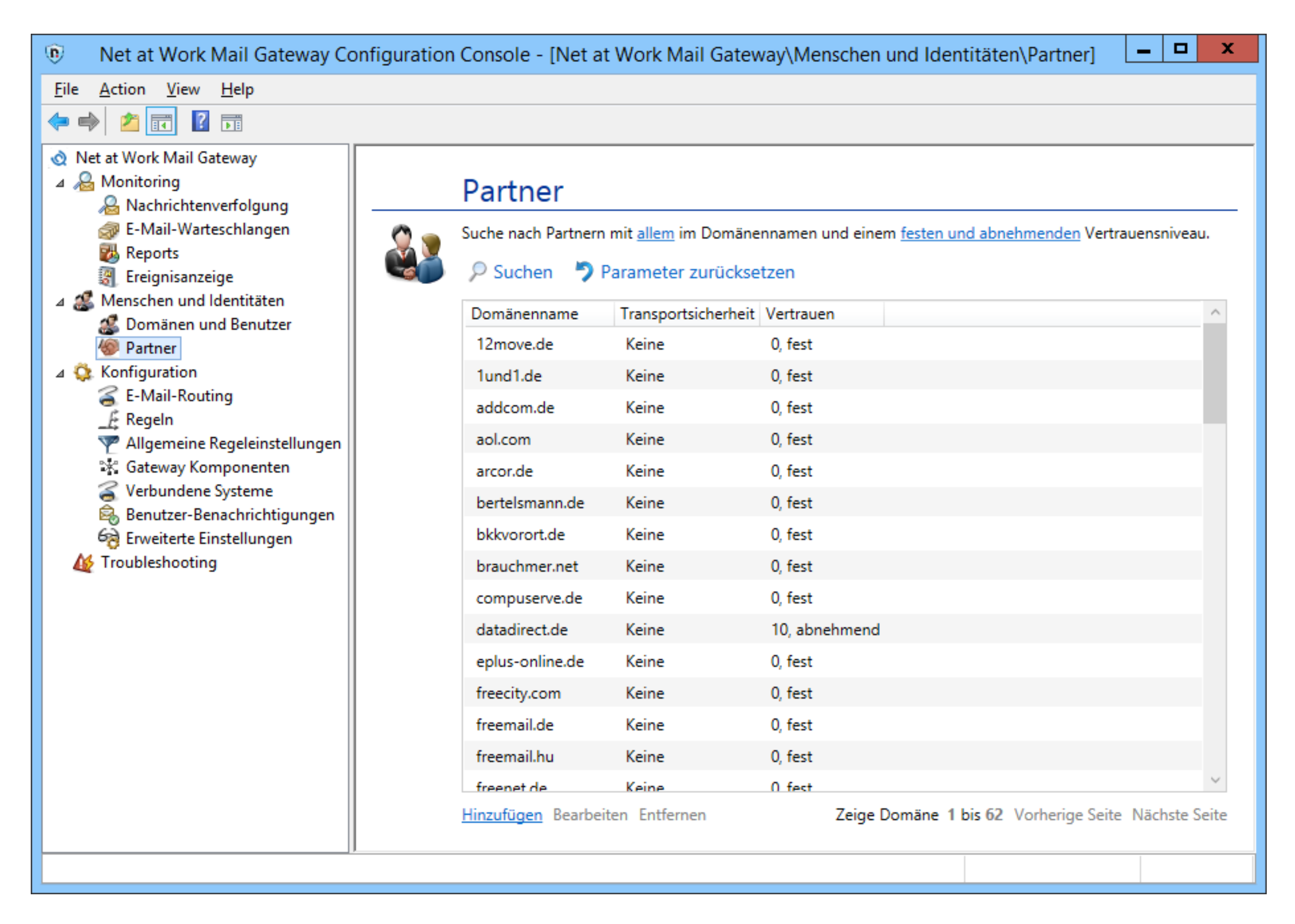


Bild 50: Die Übersicht über alle Partner

Neue Partnerdomäne

Beim Hinzufügen einer Partnerdomäne geben Sie zuerst den Domänennamen an (Bild 51). Der Domänenname muss hier mit US-ASCII-Zeichen geschrieben werden.

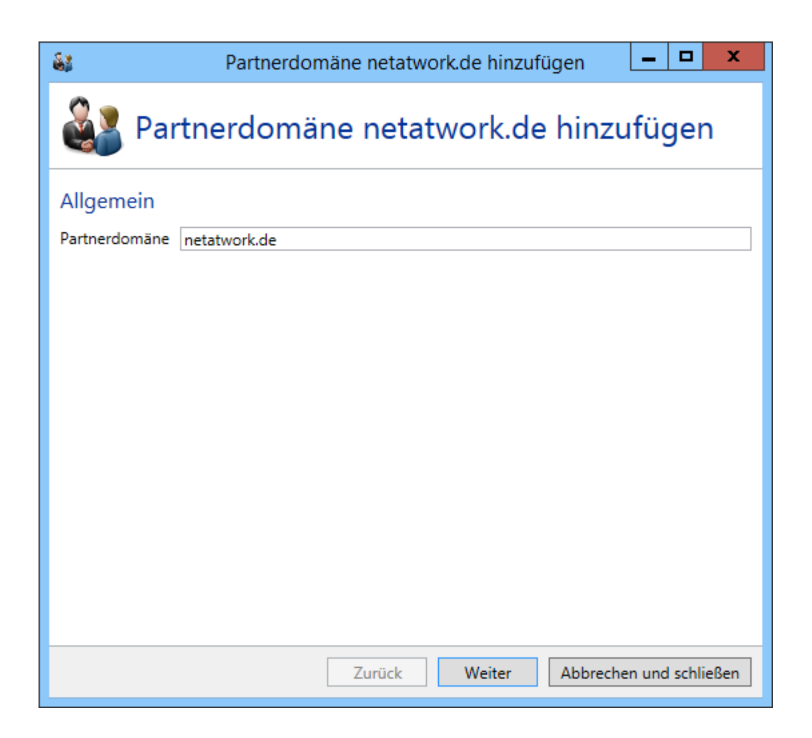


Bild 51: Der Domänenname

Die Transportsicherheit legt fest ob die Kommunikation zu den Server der Partnerdomäne verschlüsselt erfolgen muss und welche Anforderungen das verwendete Zertifikat erfüllen muss (Bild 52). Sie können hier auch weitere Zertifikate hinterlegen, die für die Transportverschlüsselung zum Zielserver eingesetzt werden können.

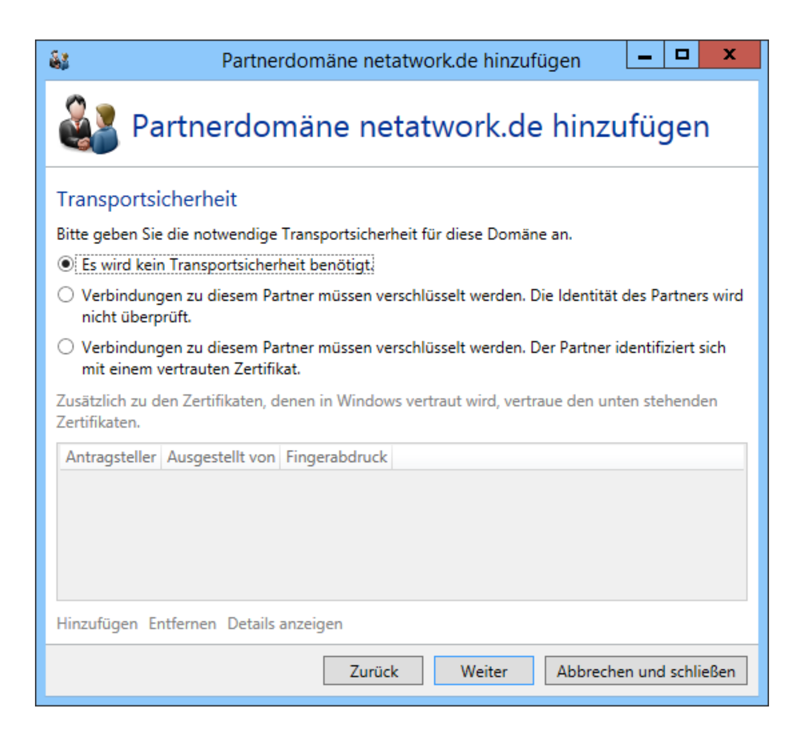


Bild 52: Transportsicherheit



Wenn Sie im E-Mail-Routing als ausgehende Zustellmethode **Zustellung über einen speziellen Server** für SMTP ausgewählt haben und in den Einstellungen für die **notwendige Transportsicherheit** einer Domäne die Verschlüsselung erzwingen, wird der Versand an diese Domäne fehlschlagen. Das Net at Work Mail Gateway kann in diesem Fall nicht sicherstellen, dass die Kommunikation bis zum E-Mail-Server des Empfängers verschlüsselt ist.

Das **Vertrauen** in eine Domäne (Bild 53) wird durch an die Domäne gesandte E-Mails stärker und nähert sich ohne weitere E-Mail-Kommunikation mit der Zeit wieder den Wert '0' an. Sie können das Vertrauen auch auf einen festen Wert einstellen. Ein positiver Wert steht in diesem Fall für Vertrauen, also Bonuspunkte, negative Werte für Misstrauen, also Malus Punkte.

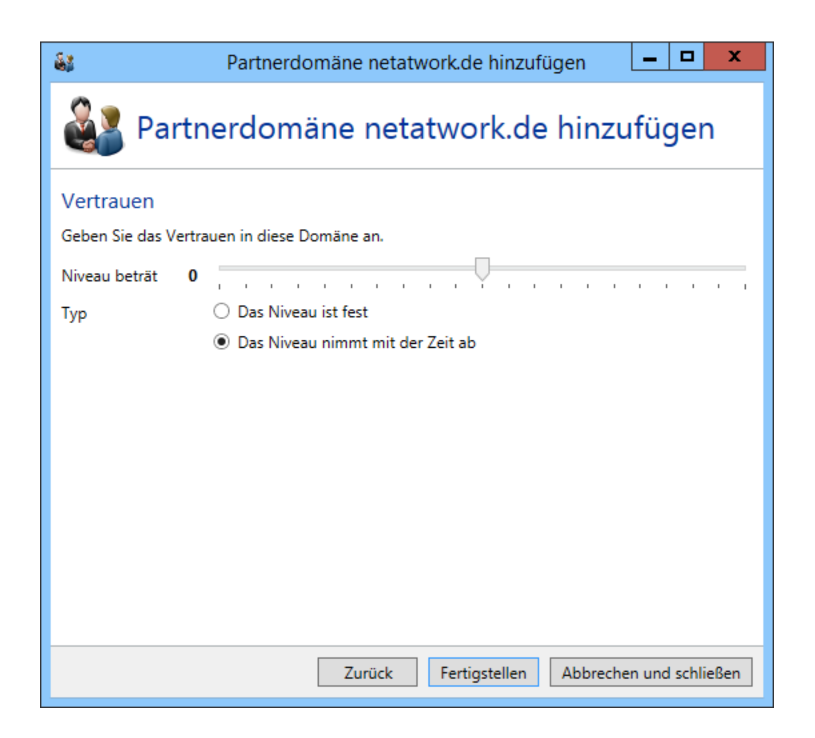


Bild 53: Das Vertrauen in eine Domäne

Partner bearbeiten

Beim Bearbeiten eines Partners können die Einstellungen aus der Domäne angepasst werden. Beim Bearbeiten eines Partners sind zusätzliche Bereiche verfügbar. Sie können individuelle Konfigurationen der Ende-zu-Ende-Verschlüsselung für jede E-Mail-Adresse der Domäne hinterlegen.



Bild 54: Domäneneintrag für einen Partner

8. Konfiguration

Unter dem Knoten **Konfiguration** der Intranet Rolle befinden sich Einstellungen für Verbindung zu anderen Rollen, Einstellungen der Datenbank sowie Benachrichtigungsadressen. (Bild 55).

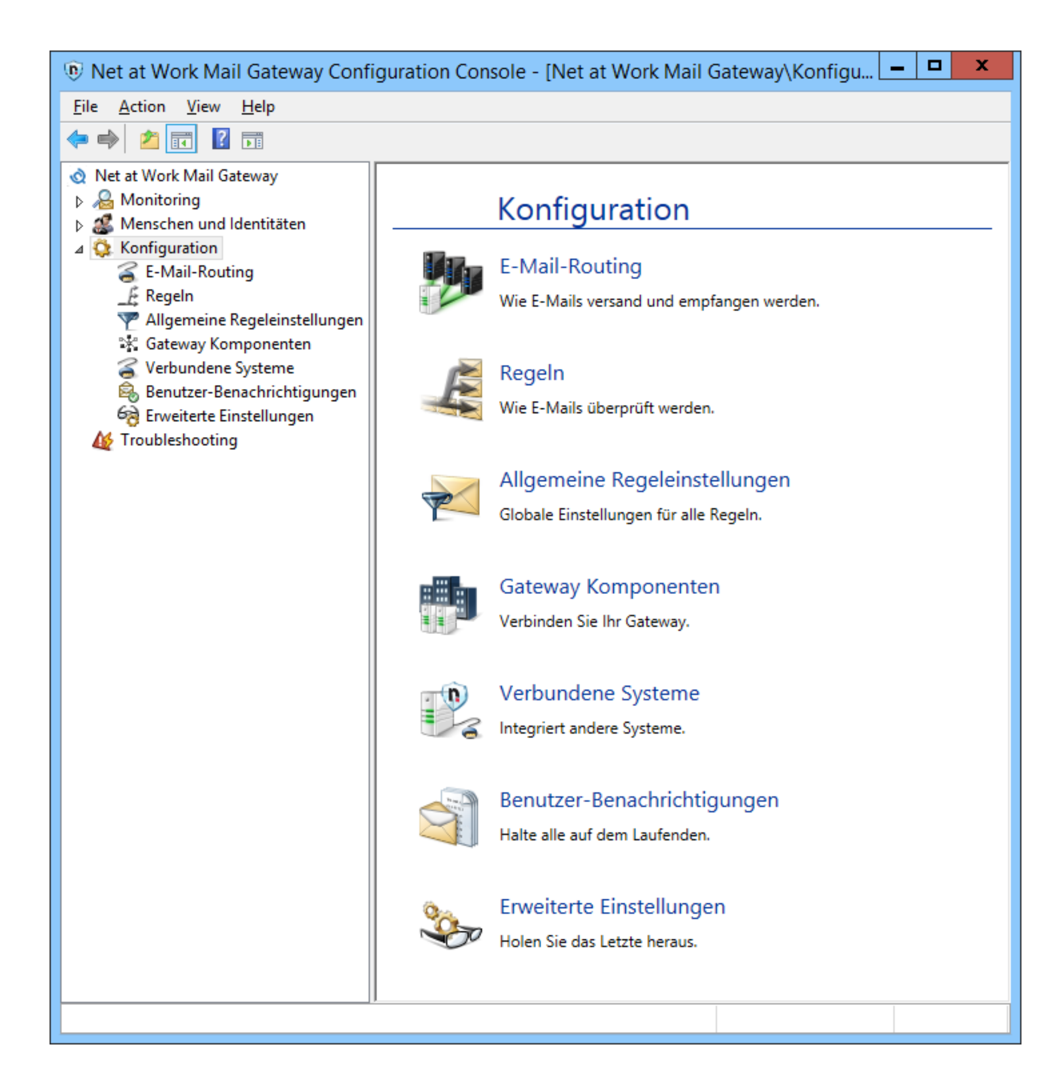


Bild 55: Einstellungen der Intranet Rolle

E-Mail-Routing

Unter dem Knoten **E-Mail-Routing** (Bild 69) befinden sich die Konnektoren für den Empfang von E-Mails der Zustellung eingehender und ausgehender E-Mails. Unter dem Punkt Empfangskonnektoren können Sie einstellen, mit welchen IP-Adressen, auf welchen Ports und mit welchen Sicherheitseinstellungen das Net at Work Mail Gateway E-Mails empfangen soll.

Des Weiteren können Sie hier De-Mail, POP3-Konnektoren, die Konnektoren für Deutschland-Online - Infrastruktur und E-Postbrief einrichten.

Mehrfach verwendete Einstellungen der Konnektoren

Einige Einstellungen werden in unterschiedlichen Konnektoren mehrfach verwendet. Diese werden in den folgenden Kapiteln erläutert.

Name

Sie müssen über das Feld **Name** jedem Konnektor einen eigenen Namen geben. Der Name muss gegenüber anderen Konnektoren aus dem gleichen Bereich eindeutig sein. Der Name dient dazu, dass Sie unterschiedliche Konnektoren unterscheiden können und kann dazu genutzt werden, die Funktion des Konnektors kurz zu beschreiben.

Bindung an Gateway Rollen

Ja nach Typ des Konnektors kann er entweder auf mehreren Gateway Rollen parallel oder aber nur auf einer einzelnen Rolle verwendet werden. Wählen Sie hier die Gateway Rollen aus, auf dem Sie den Konnektor betreiben möchten.

Kosten

Die **Kosten** werden genutzt, wenn mehrere Sendekonnektoren für die Zustellung einer E-Mail genutzt werden können. In einem solchen Fall wird der Konnektor mit den geringsten Kosten genutzt. Sollte über diesen Konnektor nicht zugestellt werden können, ist die E-Mail-Zustellung endgültig fehlgeschlagen. In diesem Fall werden keine weiteren Konnektoren mit höheren Kosten genutzt.

Verbindungssicherheit

Die Verbindungssicherheit (Bild 56) legt die Verschlüsselung der Transportverbindung fest. Der hier beschriebene Dialog wird bei den unterschiedlichen eingehenden und ausgehenden Konnektoren mehrfach benutzt. Dabei sind in einigen Konnektoren einzelne Konfigurationsoptionen ausgeblendet. Diese Abweichungen werden in den Kapiteln der entsprechenden Konnektoren aufgelistet und erklärt.



Hierbei handelt es sich um die Verschlüsselung auf dem Transportweg. Eine Ende-zu-Ende-Verschlüsselung ist hier nicht gemeint.

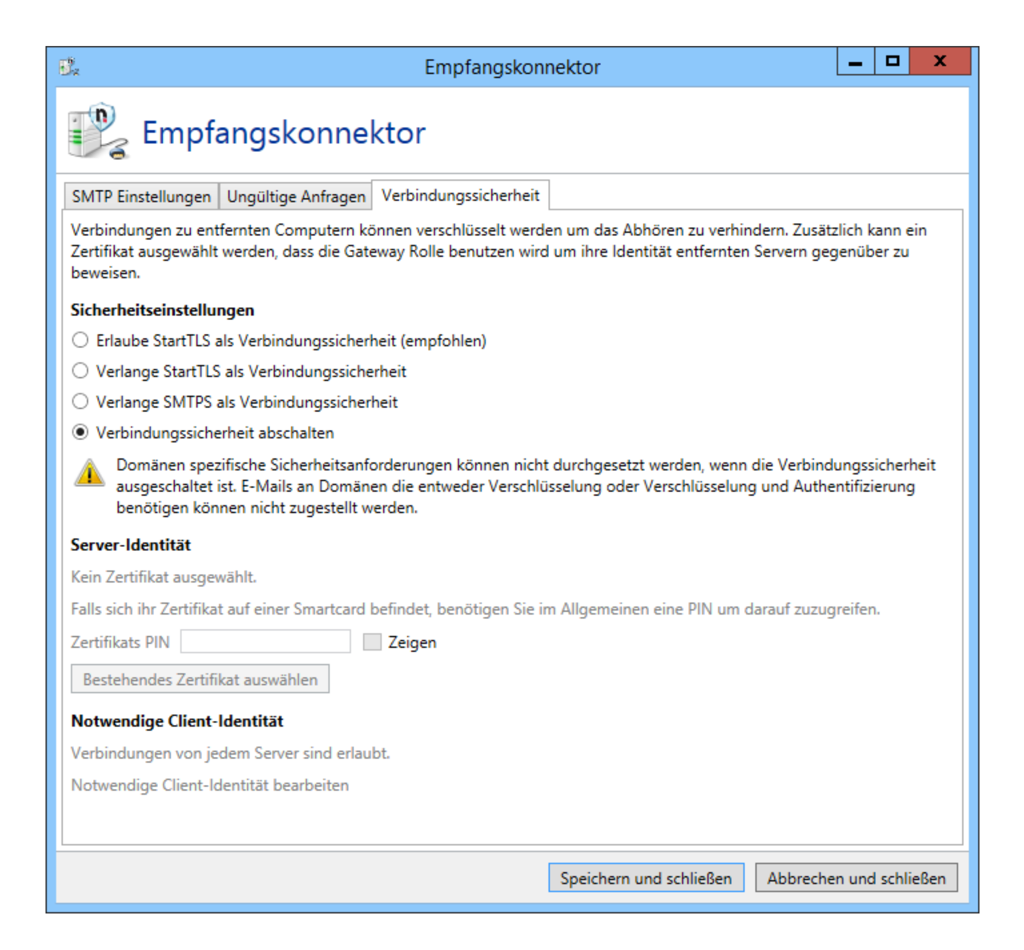


Bild 56: Einstellungen für die Verbindungssicherheit

SMTP Sicherheitseinstellungen

Im Abschnitt **Sicherheitseinstellungen** können Sie den Sicherheitsgrad für die Übermittlung von eingehenden E-Mails festlegen. Folgende Einstellungen sind möglich:

- **Verbindungssicherheit durch StartTLS erlauben (empfohlen)**
  In diesem Modus ist die Verschlüsselung der eingehenden Verbindungen möglich, aber nicht erzwungen. Dem einliefernden Server ist es freigestellt, die Verbindung via StartTLS zu verschlüsseln. In diesem Modus müssen Sie Empfangskonnektoren ein Zertifikat im Bereich Server-Identität zur Verfügung stellen. Sendekonnektoren können Sie optional ein Zertifikat im Bereich Client-Identität zur Verfügung stellen, um die Identität des sendenden Servers für den empfangenden Server sicher zu stellen.
- **Verbindungssicherheit durch StartTLS verlangen**
  Wenn Sie sicherstellen möchten, dass alle eingehenden Verbindungen über den entsprechenden Empfangskonnektor verschlüsselt werden, müssen Sie diese Option auswählen. Nun verlangt das Net at Work Mail Gateway zwingend eine verschlüsselte Verbindung vom einliefernden Server via StartTLS. Auch in diesem Modus müssen Sie dem Gateway ein Zertifikat im Abschnitt Server-Identität zur Verfügung stellen. Die Option **Verbindungssicherheit durch StartTLS verlangen** ist im ausgehenden Sendekonnektor nicht verfügbar.

- **TLS als Verbindungssicherheit nutzen**
  Mit dieser Einstellung erwartet ein SMTP Konnektor einen Verbindungsaufbau mittels SMTPS. Ein POP3 Konnektor erwartet POP3S. Verwenden Sie diese Einstellung nur dann, wenn es zwingende Gründe dafür gibt. Das StartTLS-Verfahren ist das modernere und mittlerweile gängigste Verfahren zur Verbindungsverschlüsselung. Normalerweise wird für SMTPS ein separater Port (üblicherweise 465) verwendet, da die Verbindung automatisch verschlüsselt erwartet wird, ähnlich wie bei HTTPS über den Port 443.
- **Verbindungssicherheit abschalten**
  Mit dieser Einstellung werden eingehende Verbindungen niemals verschlüsselt. Das Net at Work Mail Gateway bietet dann einliefernden Servern keine Verbindungssicherheit an.



SMTPS auf Port 25 ist nicht RFC konform. Nutzen Sie stattdessen einen eigenen Empfangskonnektor, den Sie auf den Port 465 legen.



Das notwendige Verschlüsselungsniveau für Verbindung mit StartTLS oder SMTPS beträgt mindesten 128 Bit. Verbindungen mit einer kleineren Verschlüsselungsstärke werden nicht angenommen.

Server- oder Client-Identität

Für die Verschlüsselung der Transport Verbindung werden SSL-Zertifikate benötigt. Der empfangende E-Mail-Server benötigt zwingend ein Zertifikat als Server-Identität, um die Verschlüsselung der Verbindung zu ermöglichen. Der sendende E-Mail-Client kann mit einem Zertifikat seine eigene Client-Identität belegen.

- **Server-Identität**
  Ein SSL-Zertifikat im Empfangskonnektor wird genutzt, um eine Verbindungssicherheit bereitstellen zu können. Mithilfe des Zertifikats als Server-Identität beim empfangenden E-Mail-Server wird die Verschlüsselung durch StartTLS bzw. TLS ermöglicht. Ohne Zertifikat muss die Verschlüsselung für eingehende Verbindungen deaktiviert werden.
- **Client-Identität**
  Ein SSL-Zertifikat in SMTP Sendekonnektoren wird genutzt, um die Identität des sendenden E-Mail-Servers sicher zu stellen. Auch ohne Zertifikat als Client-Identität kann die Verbindungssicherheit durch StartTLS bzw. TLS genutzt werden, da das Zertifikat der Server-Identität des empfangenden Servers für die Verschlüsselung der Transportverbindung ausreicht.



Beim Hinzufügen eines Zertifikats für die Transport Verschlüsselung durch StartTLS benötigt die Gateway Rolle Leserechte auf den privaten Schlüssel. Diese Rechte für die Rolle werden automatisch erteilt. Sie müssen allerdings einmal die Gateway Rolle stoppen und wieder starten damit diese Änderung wirksam wird und die Gateway Rolle Leserechte auf dem privaten Schlüssel des genutzten Zertifikats erhält. Es erscheint auch ein entsprechender Warnhinweis in der Oberfläche (Bild 57).

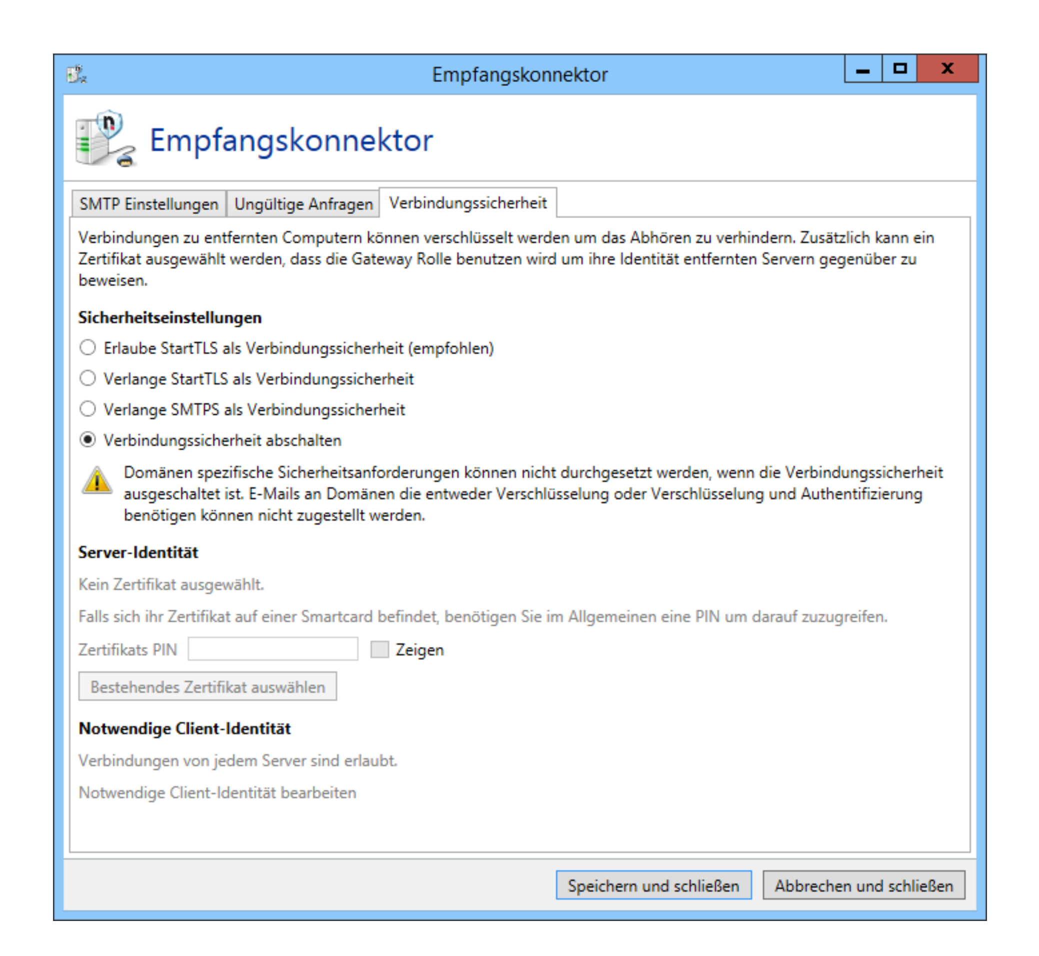


Bild 57: Starten Sie die Gateway Rolle neu, nachdem Sie ein neues Zertifikat als Server-Identität ausgewählt haben

Nach der Auswahl des Zertifikats müssen Sie ggf. einen PIN-Code in das Feld **Zertifikats PIN (optional)** eingeben, falls der Zertifikatsspeicher die Zertifikate mit einem solchen geschützt hat.



Bitte kontrollieren Sie die Eingabe Ihrer PIN sehr sorgfältig, da viele der durch einen PIN-Code geschützten Zertifikate durch dreimalige Falscheingabe unwiderruflich zerstört werden.

Wird für Verbindungen SSL erzwungen, so können Sie im Punkt **Notwendige Client-Identität** noch einschränken, welche Clients sich verbinden dürfen indem Sie den Zugriff nur erlauben sofern sich die Gegenstelle mit einem passenden Zertifikat authentifiziert (Bild 58):

- **Erlaube Verbindungen von jedem Server**
  Jeder Server darf sich verbinden.
- **Verlange ein Zertifikat**
  Das von der Gegenstelle vorzulegende Zertifikat hängt vom hier ausgewählten Zertifikat ab: Bei einem Zwischen- oder Stammzertifikat muss sich die Gegenstelle mit einem Zertifikat ausweisen,

das das gewählte Zertifikat in der Zertifikatskette hat. Bei einem Endzertifikat muss sich die Gegenstelle mit exakt diesem Zertifikat ausweisen.

- **Verlange ein vertrautes Zertifikat**
  Die Zertifikatskette des vorgelegten Zertifikats muss über die Zertifikate des Windows-Zertifikatsspeichers auflösbar sein.

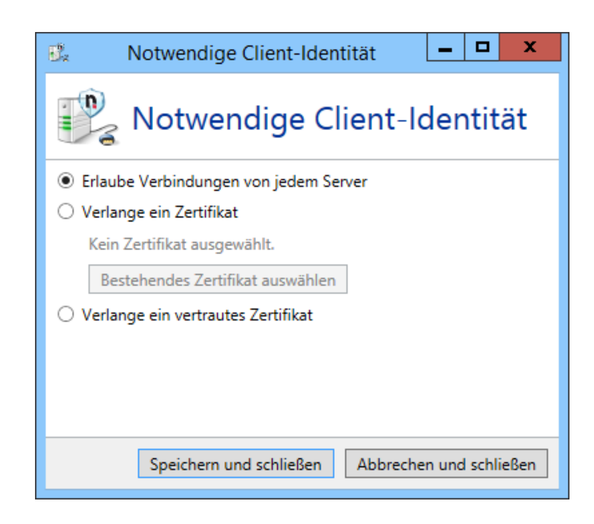


Bild 58: Festlegung der notwendigen Client-Identität

DNS Routing Einschränkungen durch Konnektor Namensräume

Ein Sendekonnektor kann auch so konfiguriert werden, dass er E-Mails nur für einen Teilbereich des zur Verfügung stehenden DNS-Namensraums zustellt. Sollten mehrere Konnektoren auf eine E-Mail zutreffen, so werden die im Konnektor eingestellten Kosten berücksichtigt. Der Konnektor mit den geringsten Kosten wird die E-Mail versenden.

Standardmäßig wird in einem neuen Konnektor ein Namensraum von "*" als Absenderdomäne und "*" als Empfängerdomäne automatisch angelegt. Dadurch ergibt sich bei einem neuen Konnektor keine Einschränkung im DNS Namensraum, da der Platzhalter "*" jedem möglichen Namen entspricht. Falls der von Ihnen angelegte Konnektor nicht alle Domänen verwalten soll, müssen Sie den Standard Namensraum löschen und durch einen anderen Namensraum ersetzen.

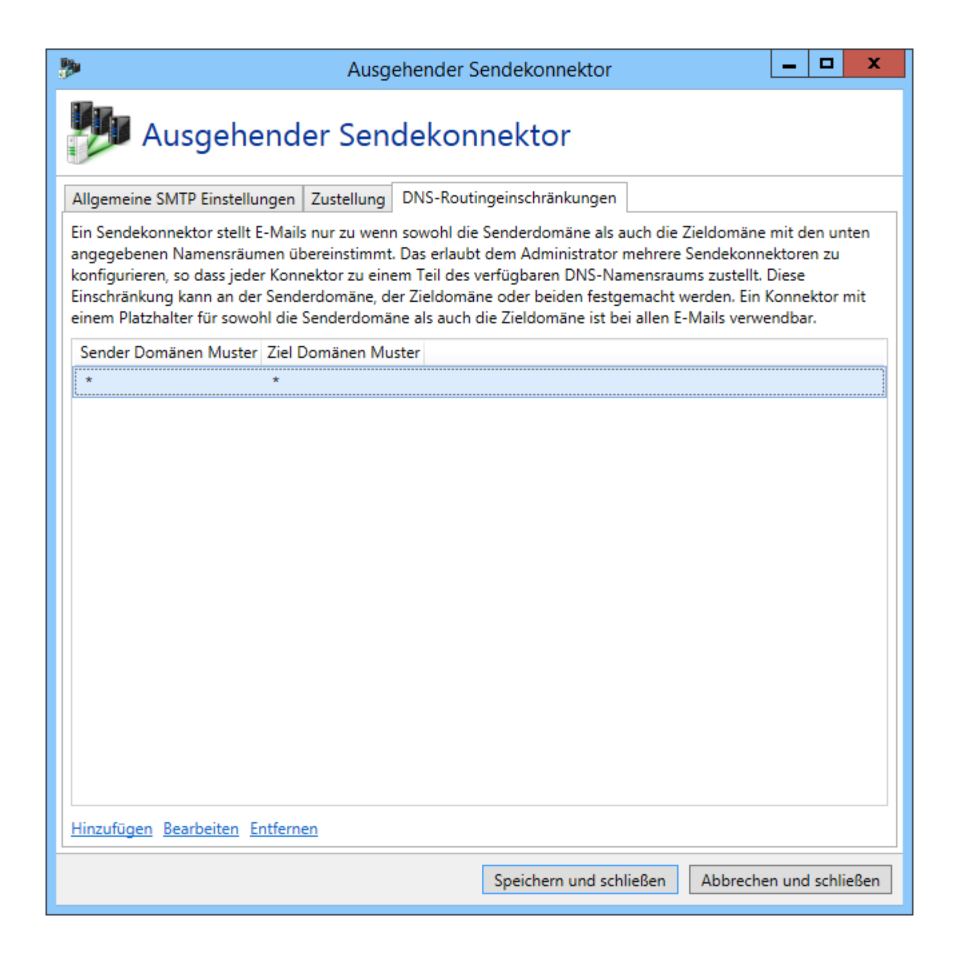


Bild 59: Die Konnektor-Namensräume bestimmen, welche Absender- oder Empfänger-Domänen von einem Konnektor verwaltet werden

Ein Konnektor-Namensraum (Bild 60) besteht aus einem Muster für sowohl die "Sender Domäne" als auch "Ziel Domäne". Dieses Muster darf auch Platzhalter ('*' und '?') enthalten.

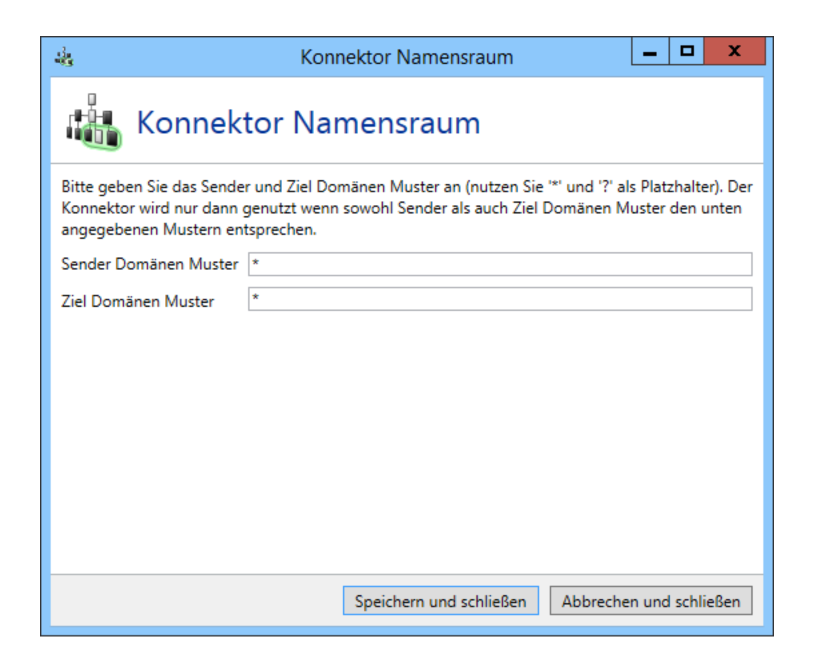


Bild 60: Definieren Sie die einzelnen Namensräume für den Konnektor

Beispiel: Um einen ausgehenden Sendekonnektor zu bauen, der nur E-Mails von der Domäne "example.com" an die Domäne "netatwork.de" versendet, müssen folgende Einstellungen getätigt werden.

Sender Domänen Muster	Ziel Domänen Muster
example.com	netatwork.de

Smarthost: E-Mail-Zustellung über dedizierten Server

Ein Smarthost ist ein dedizierter Server für die Zustellung von E-Mails. Smarthosts stehen zum Beispiel bei Ihrem Internet Provider oder auch im eigenen Firmennetz, falls nur über diesen Server E-Mails versendet werden dürfen.

Geben Sie in der Seite **Dedizierter Server** die IP-Adresse oder den Servernamen und den Port des dedizierten Servers ein (Bild 61). Dies ist in der Regel die IP-Adresse bzw. der Servername des nächsten Mailsystems für E-Mails.

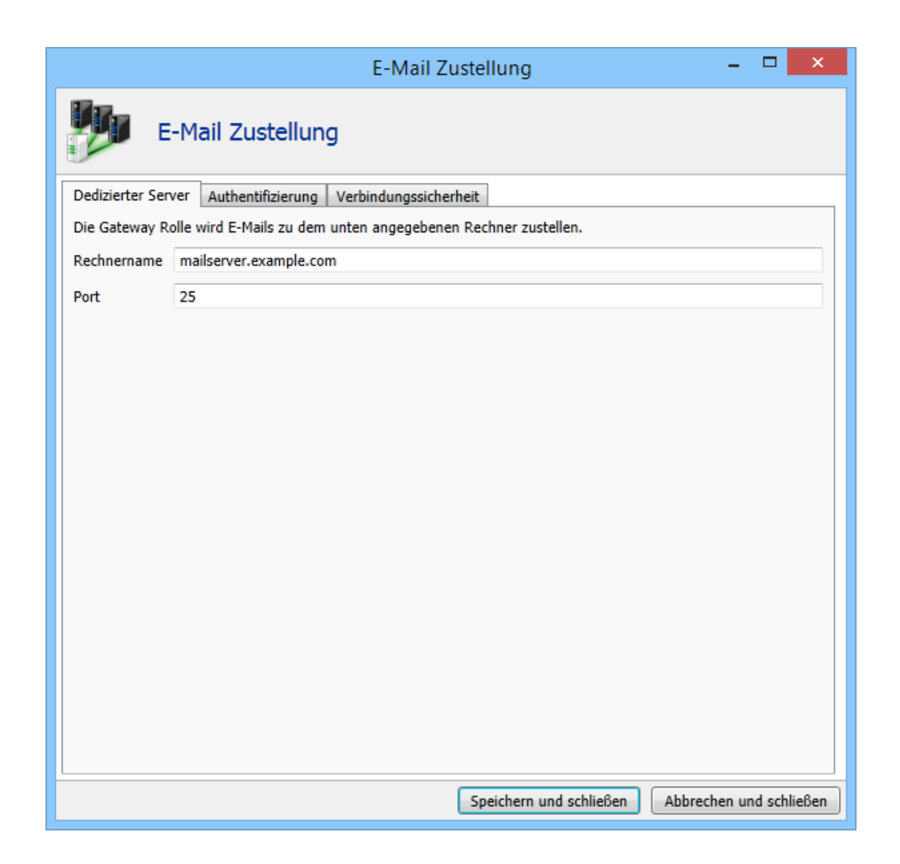


Bild 61: Verbindungseinstellungen für den dedizierten Server



Wir empfehlen, Adressen nach Möglichkeit nicht als IP-Adresse, sondern mit Servernamen einzugeben.

Für externe Smarthosts, wie zum Beispiel den Ihres Providers, werden häufig Benutzername und Kennwort für die Authentifizierung verlangt. Diese können Sie auf der Registerkarte **Authentifizierung** angeben (Bild 62).

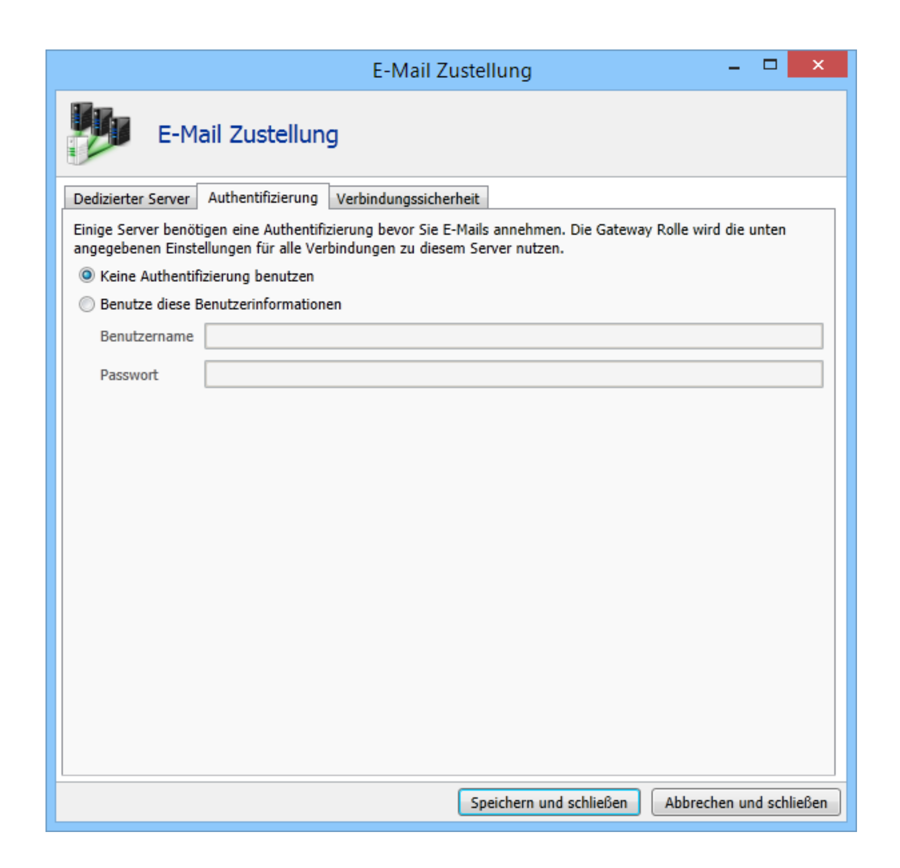


Bild 62: Hier können Sie ggf. Anmeldeinformationen für den dedizierten Server hinterlegen



Das Net at Work Mail Gateway unterstützt als Authentisierungsverfahren die Methode „Basic“. Bei dieser Methode werden Benutzername und Kennwort unverschlüsselt über das Internet übertragen. Sofern Ihr Provider das unterstützt, sollten Sie die Verbindungssicherheit für die Verbindungen aktivieren.

Die Optionen für die Verbindungssicherheit zu Smarthosts ist, wie im Kapitel Verbindungssicherheit beschrieben, zu konfigurieren. Ausgehende SMTP Sendekonnektoren nutzen die zertifikatsbasierte Identität nur als Client-Identität.



Wenn Sie die ausgehenden E-Mails über einen weiteren Smarthost verschicken und in den Vertrauensstellungen bei einer Domäne die Verschlüsselung erzwingen, wird der Versand an diese Domäne fehlschlagen, wenn der Smarthost für die ausgehenden E-Mails keine Verschlüsselung unterstützt. Sie müssen also dafür sorgen, dass der Smarthost für die ausgehenden E-Mails StartTLS immer unterstützt.

Eingehende Zustellung

Unter dem Punkt **Eingehende Zustellung** legen Sie fest, an welche Server E-Mails von externen E-Mail-Servern weitergeleitet werden. Externe E-Mail-Server sind dabei alle Server, die nicht in der Liste der internen E-Mail-Server aufgeführt sind.

Die eingehende Zustellung von E-Mails kann hier entweder über das "Warteschlangensystem" erfolgen oder wie bei einem Proxy auch direkt zum internen E-Mail-Server zugestellt werden. Dabei ist zu beachten, dass die Zustellung über Warteschlangen mehrere Smarthost und die direkte Zustellung nur einen Smarthost unterstützt. Genauer werden die Unterschiede in den folgenden Kapiteln erläutert.

Zustellung über Warteschlangen

In diesem Modus wird das Net at Work Mail Gateway die E-Mail nach dem Empfang zunächst in eine Warteschlange legen und dann erst an den oder die konfigurierten Smarthosts weiterleiten. Für den erfolgreichen Empfang der E-Mail ist es nicht relevant, ob der nächste Smarthost erreichbar ist oder nicht.



Auch im Warteschlangenmodus wird die E-Mail noch während der Übertragung von NoSpamProxy auf Viren und den Spamgehalt überprüft und ggfs. abgewiesen.

Eingehender Sendekonnektor über Warteschlangen

Wenn Sie für den eingehenden Sendekonnektor den Warteschlangenmodus auswählen, wird eine eventuell existierende Konfiguration durch den neu konfigurierten Warteschlangenmodus ersetzt. Wenn Sie zum Warteschlangenmodus wechseln, wird sofort der erste SMTP Konnektor konfiguriert. Die Schritte dazu werden in den folgenden Kapiteln erläutert. Falls Sie weitere Konnektoren hinzufügen möchten, können Sie in der Übersicht **Neuen Konnektor hinzufügen** wählen.

Allgemeine Einstellungen

Geben Sie einen Namen ein und wählen Sie den oder die Gateway Rollen aus. Legen Sie anschließend die Kosten des Konnektors fest.

SMTP Verbindungen

Unter den SMTP-Verbindungen können Sie mehrere Smarthosts konfigurieren. Es wird versucht, die E-Mail nacheinander an einen der konfigurierten Smarthosts zuzustellen. Die Reihenfolge ist hierbei weder konfigurierbar noch vom Benutzer beeinflussbar. Sobald ein Smarthost die E-Mail empfängt, ist die E-Mail erfolgreich zugestellt.

Konfiguration eines Smarthosts

Die Konfiguration eines Smarthosts für die eingehende Zustellung läuft ab, wie im Kapitel Smarthost: E-Mail-Zustellung über dedizierten Server beschrieben. Der eingehende Sendekonnektor nutzt in der Verbindungssicherheit eine Client-Identität.

DNS Routing Einschränkungen

Die Einschränkungen für den von dem Konnektor verwalteten Namensraum definieren Sie unter **DNS Routing Einschränkungen**. Die Konfiguration der Einschränkungen für die eingehende Zustellung läuft ab, wie im Kapitel DNS Routing Einschränkungen durch Konnektor Namensräume beschrieben.

Direkte Zustellung

Durch die "Direkte Zustellung" konfigurieren Sie, dass sich das Net at Work Mail Gateway bei eingehenden E-Mails wie ein SMTP-Proxy verhalten soll. Bei dieser Einstellung ist darauf zu achten, dass der konfigurierte Smarthost immer verfügbar ist um die E-Mails anzunehmen. Wenn das nicht der Fall sein sollte, wird das Mail Gateway die E-Mail nicht annehmen. Der einliefernde Smarthost wird die Zustellung zu einem späteren Zeitpunkt erneut versuchen. Des Weiteren ist es in diesem Modus nur möglich, einen eingehenden E-Mail-Server anzugeben.

Die Konfiguration der direkten eingehenden Zustellung läuft ab, wie im Kapitel Smarthost: E-Mail-Zustellung über dedizierten Server beschrieben.

Ausgehende Zustellung

Unter dem Punkt **Ausgehende Zustellung** legen Sie fest, wie E-Mails von einem der internen E-Mail-Server an einen externen Server versendet werden. Interne E-Mail-Server sind dabei alle Server, die sich in der Liste der internen E-Mail-Server befinden.

SMTP Konnektoren

Für die Zustellung zu normalen externen SMTP-Servern werden die SMTP Konnektoren eingesetzt. Über diese kann entweder eine direkte Zustellung zu den Ziel SMTP-Server konfiguriert werden oder eine Zustellung über einen dedizierten Server (Smarthost), der alle E-Mails des Konnektors annimmt, um sie zur Zustellung weiter zu leiten.

Allgemeine Einstellungen

Geben Sie einen Namen ein und wählen Sie den oder die Gateway-Rollen aus. Legen Sie anschließend die Kosten des Konnektors fest. Wählen Sie danach als **Routing Methode** entweder die Direkte Zustellung (DNS) oder die Auslieferung über einen dedizierten Server (Smarthosts).

Zustellung - Direkte Zustellung (DNS)

Bei der direkten Zustellung über DNS Server wird versucht, die E-Mails direkt zu Ihren Ziel-Servern zuzustellen. Der ausgehende Sendekonnektor nutzt bei der direkten Zustellung in der Verbindungssicherheit eine Client-Identität.

Zustellung - Dedizierte Server (Smarthosts)

Die Konfiguration eines Smarthosts für die eingehende Zustellung läuft ab, wie im Kapitel Smarthost: E-Mail-Zustellung über dedizierten Server beschrieben. Die Verbindungssicherheit für die Verbindung zu jeweiligen Smarthost besitzt die gleichen Optionen und Einschränkungen wie im Kapitel Zustellung - Direkte Zustellung (DNS) beschrieben.

DNS Routing Einschränkungen

Die Einschränkungen für den von dem Konnektor verwalteten Namensraum definieren Sie unter **DNS Routing Einschränkungen**. Die Konfiguration der Einschränkungen für die eingehende Zustellung läuft ab, wie im Kapitel DNS Routing Einschränkungen durch Konnektor Namensräume beschrieben.

De-Mail-Konnektor

Um E-Mails in das De-Mail-Netzwerk zu senden, stehen Ihnen mehrere De-Mail-Dienstanbieter bereit. Diesen können Sie auf der ersten Seite des Dialogs **Ausgehender Sendekonnektor** auswählen. (Bild 63).

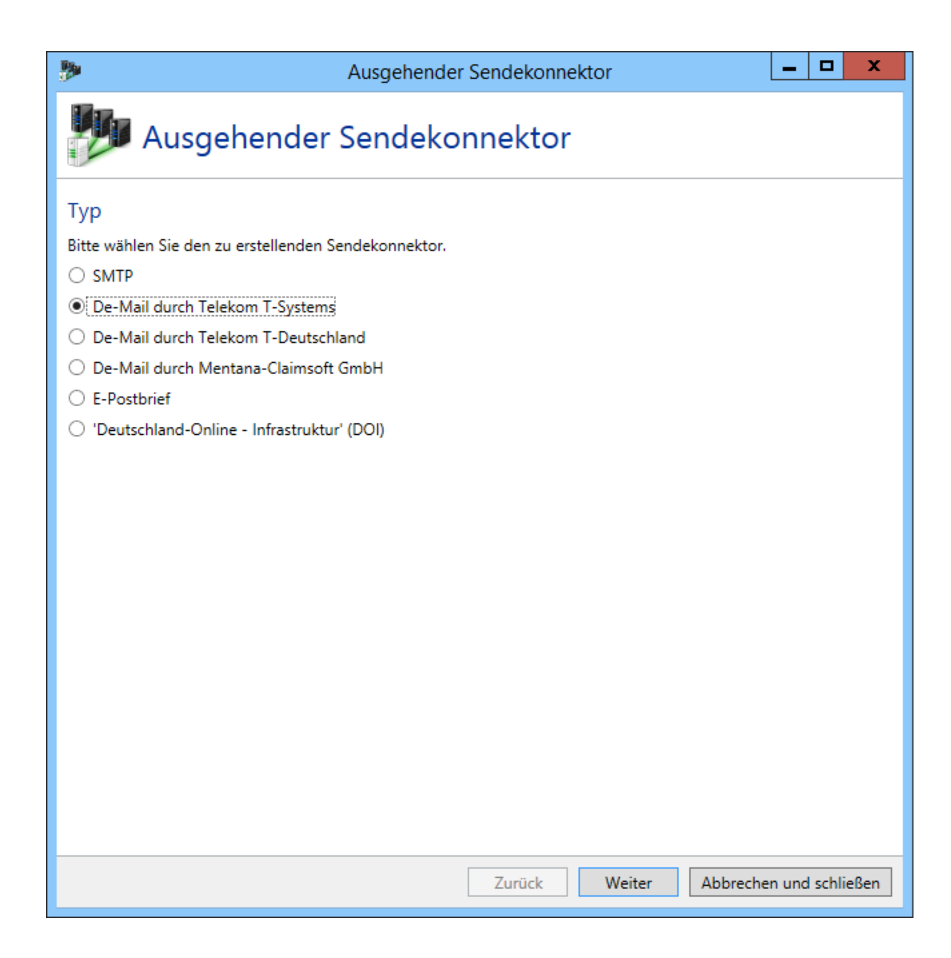


Bild 63: Die Auswahl des Konnektortyps

Geben Sie einen Namen ein und wählen Sie den oder die Gateway-Rollen aus. Auf der nächsten Seite legen Sie dann fest, welche eigenen Domänen diesem Konnektor zugeordnet sind. Mindestens eine Domäne müssen Sie hier auswählen. (Bild 64) eine oder mehrere Ihrer eigenen Domänen hinzufügen.

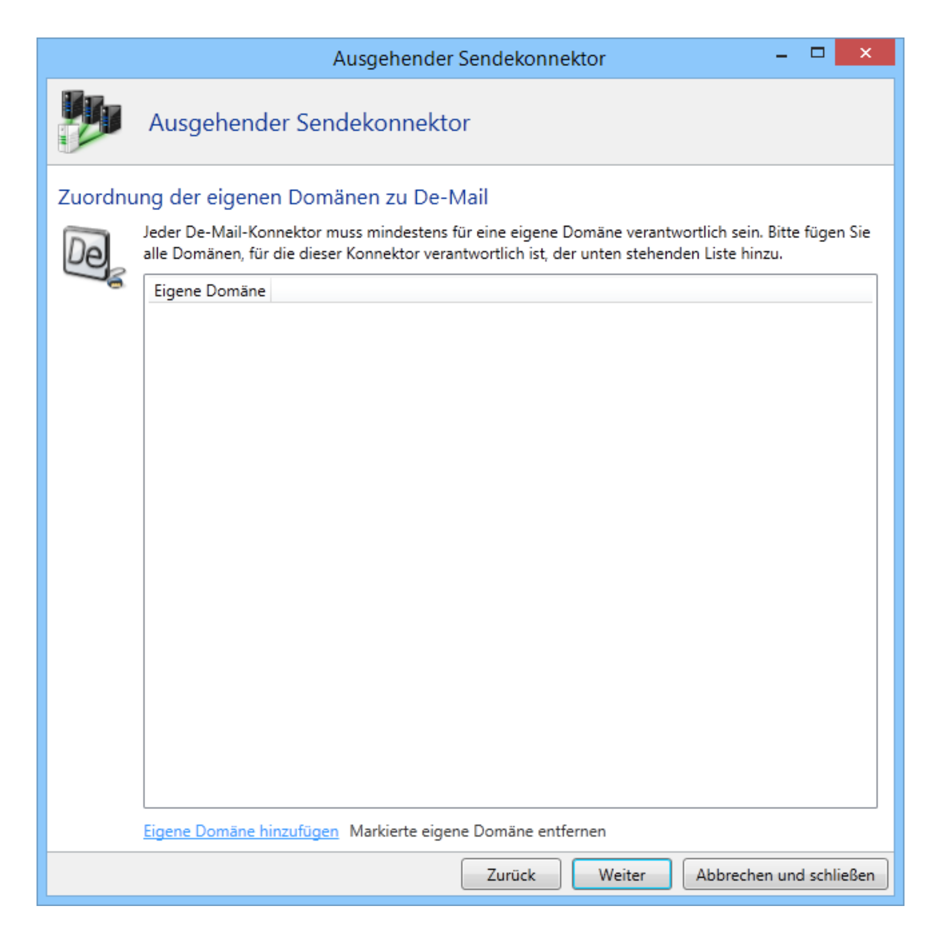


Bild 64: Zuordnung der eigenen Domänen zu De-Mail

Falls Sie nur einen ausgehenden De-Mail-Sendekonnektor konfigurieren, fügen Sie diesem bitte alle eigenen Domänen hinzu. Bei mehreren De-Mail-Sendekonnektoren müssen Sie die passenden eigenen Domänen dem jeweiligen Konnektor hinzufügen, damit das Net at Work Mail Gateway entscheiden kann über welchen De-Mail-Konnektor eine E-Mail versandt wird.

Bei einem De-Mail-Sendekonnektor für die Telekom oder T-Systems müssen Sie noch ein Zertifikat für die Verbindung auswählen. (Bild 65)

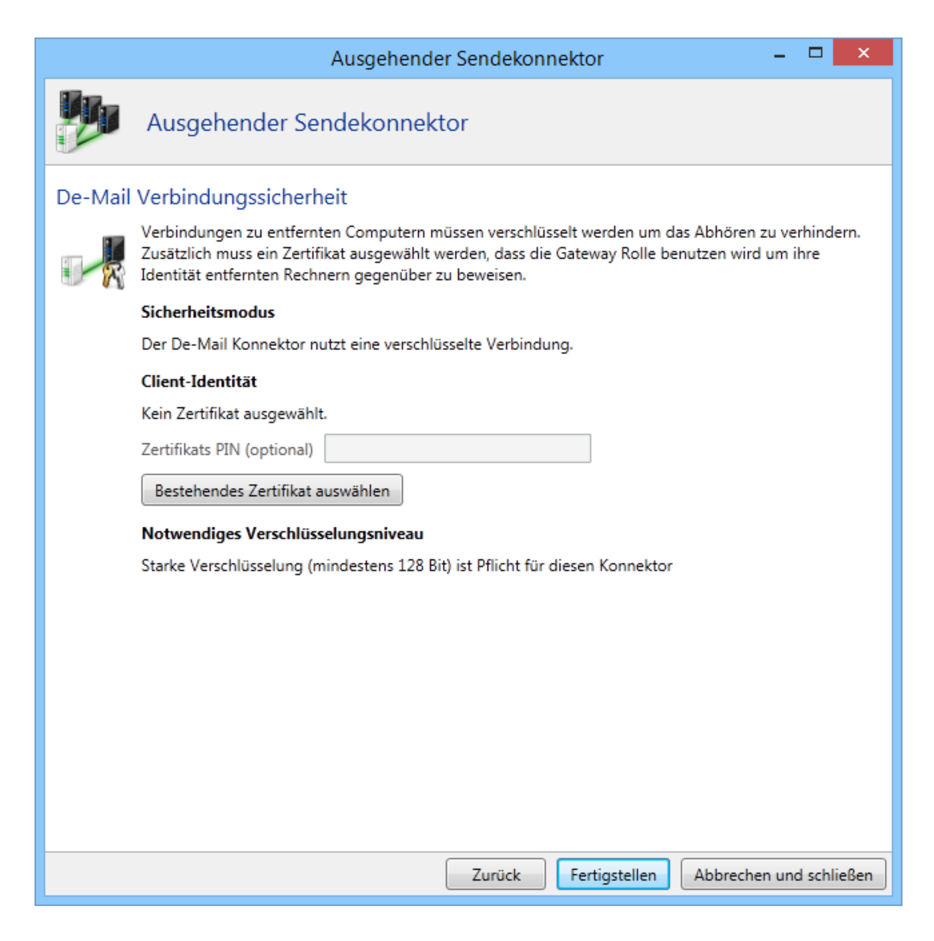


Bild 65: Die Verbindungssicherheit eines De-Mail-Konnektors

Die Verbindungssicherheit eines Mentana-Claimsoft De-Mail-Konnektors benötigt keine zusätzlichen Einstellungen. Die Verbindungssicherheit wird über den Mentana-Claimsoft De-Mail DMDA Webservice-Proxy sichergestellt.

E-Postbrief Konnektor

Die Deutsche Post ermöglicht mit dem E-Postbrief eine verbindliche, vertrauliche und verlässliche Kommunikation. Einzelheiten zu diesem Angebot finden Sie unter der Adresse http://www.epostbrief.de. Firmen haben die Möglichkeit der direkten Anbindung an die Infrastruktur der Deutschen Post über ein sogenanntes Individualkommunikationsgateway (IKG). Das IKG wird in Ihrem Unternehmen installiert und fungiert als SMTP Endpunkt für das E-Mail-Routing ins Netz der Deutschen Post.

Der E-Postbrief Konnektor übernimmt das automatische Routing von E-Mails an ein IKG. Außerdem wird sichergestellt, dass E-Postbriefe nur von dem IKG aus angenommen werden. Dadurch wird gewährleistet, dass nicht eine reguläre E-Mail, die aus dem Internet empfangen wurde, als E-Postbrief ausgegeben werden kann.

Erstellen Sie im Knoten E-Mail-Routing unter dem Punkt **Ausgehende Zustellung** einen neuen Konnektor. Im folgenden Dialog wählen Sie als Typ **E-Postbrief** und klicken dann auf **Weiter**. Auf der folgenden Seite können Sie für verschiedene interne Domänen festlegen, an welches IKG E-Postbriefe

von dieser Domain geschickt werden. Klicken Sie auf **Fertigstellen**, um den Konnektor zu erstellen (Bild 66).

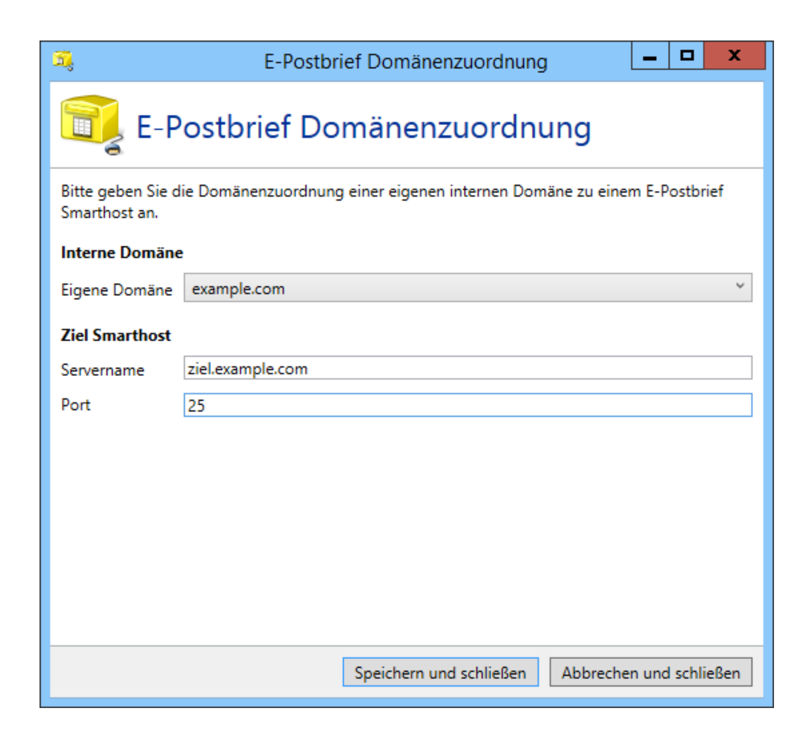


Bild 66: Die Konfiguration für die Zustellung von E-Postbriefen

Deutschland-Online - Infrastruktur Konnektor

Das Deutschland-Online - Infrastruktur (DOI) Projekt wird unter anderem von Kommunen zur sicheren Übertragung von Nachrichten verwendet. Wenn Sie kein Mitglied im DOI Projekt sind, dann haben Sie für diesen Konnektor keine Verwendung und können dieses Kapitel überspringen.

Der DOI-Konnektor lädt automatisch die aktuelle Tabelle aller Teilnehmer herunter und leitet E-Mails an andere Teilnehmer über das sichere DOI Netzwerk.

Um die Zustellung in das DOI Netzwerk zu aktivieren, erstellen Sie im Knoten E-Mail-Routing unter dem Punkt **Ausgehende Zustellung** einen neuen Konnektor. Im folgenden Dialog wählen Sie als Typ **Deutschland-Online - Infrastruktur (DOI)** und klicken dann auf **Weiter**. Im nächsten Schritt müssen Sie die FTP- oder Web-Adresse eintragen, von der Sie die Mailer-Tabelle beziehen. Geben Sie dann unter **Authentifizierung** Ihren Benutzernamen und Ihr Kennwort an. Abschließend wählen Sie für die Kosten einen kleineren Wert als den, der bei dem Standard Konnektor für ausgehende E-Mails eingetragen ist. So ist gewährleistet, dass nicht der Standard Routing-Konnektor das Routing für diese E-Mails übernimmt. Klicken Sie auf **Weiter**, wenn Sie alle Eingaben durchgeführt haben (Bild 67).

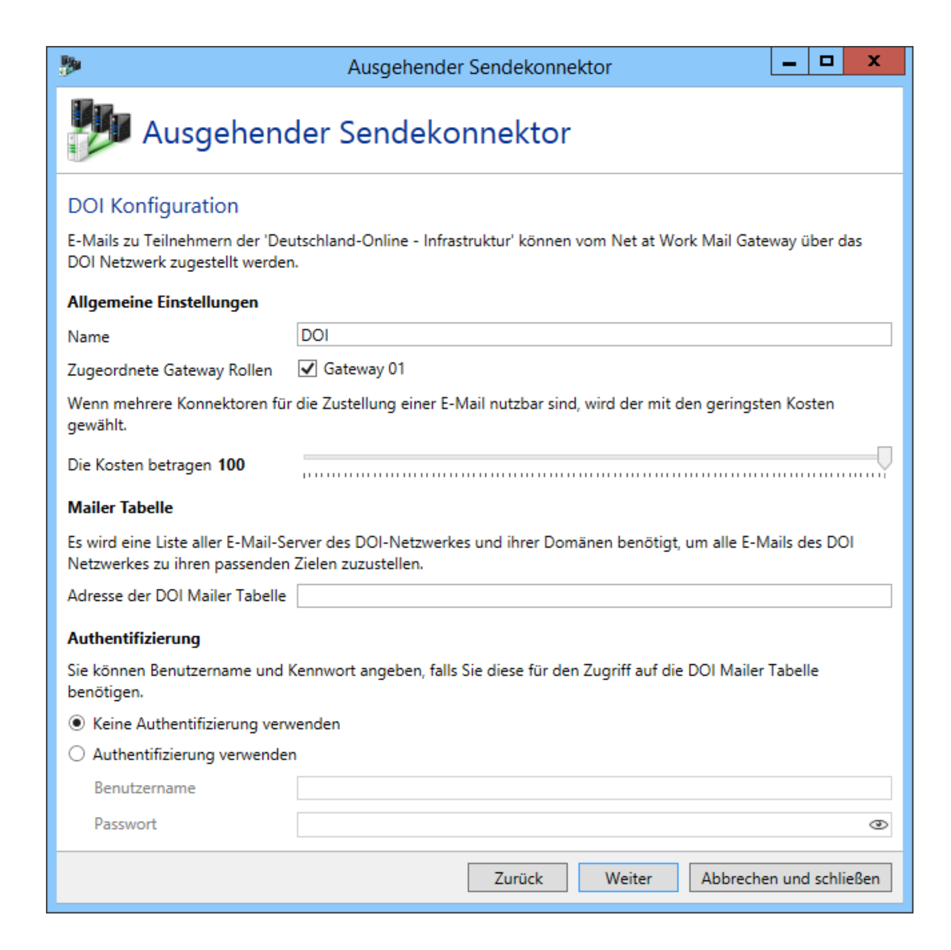


Bild 67: Die Konfiguration für die Zustellung in das Netz von Deutschland-Online - Infrastruktur

Auf der Seite **DOI Zustellung** können Sie das Verhalten für ungültige Absender konfigurieren. Absender sind immer dann ungültig, wenn die Absenderdomäne nicht Teil des DOI-Netzwerkes ist. Diese E-Mails dürfen dann nicht über das DOI Netz zugestellt werden. Sie können nun wählen, ob diese E-Mails an den Absender zurückgehen oder ob sie über einen anderen Konnektor mit höheren Kosten gesendet werden. Des Weiteren können Sie auf dieser Seite festlegen, wie E-Mails zugestellt werden. Einerseits können die E-Mails direkt zugestellt werden, andererseits, und das ist die empfohlene Möglichkeit, kann ein Smarthost verwendet werden. Ein solcher Smarthost wird vom DOI Netz zur Verfügung gestellt.

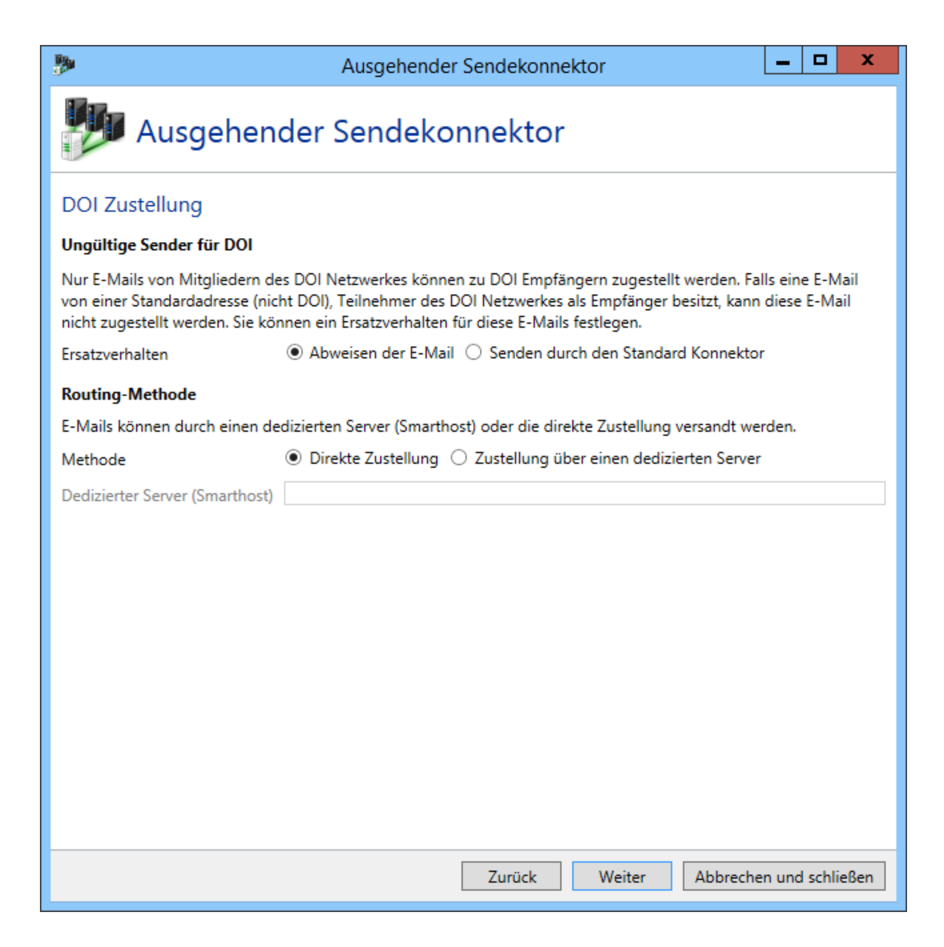


Bild 68: Erweiterte Zustelloptionen für das DOI Netz



Bei einer Zustellung über das DOI Netzwerk wird die zugestellte E-Mail in der Nachrichtenverfolgung als "nicht verschlüsselt" beschrieben. Die E-Mail wird in diesem Fall über das DOI Netzwerk verschlüsselt und ist damit abhörsicher zugestellt. Diese Absicherung wird unter der Transportsicherheit nicht aufgeführt.

Empfangskonnektoren

Es können mehrere Empfangskonnektoren konfiguriert werden, um auf unterschiedliche Netzwerkkarten E-Mails zu empfangen, aber auch um unterschiedliche Sicherheitsanforderungen für den E-Mail-Verkehr zu realisieren. Wenn Sie die Connector Services von enQsig oder enQsig CS lizenziert haben, stehen Ihnen zusätzlich Konnektoren für De-Mail und POP3 Postfächer zur Verfügung.

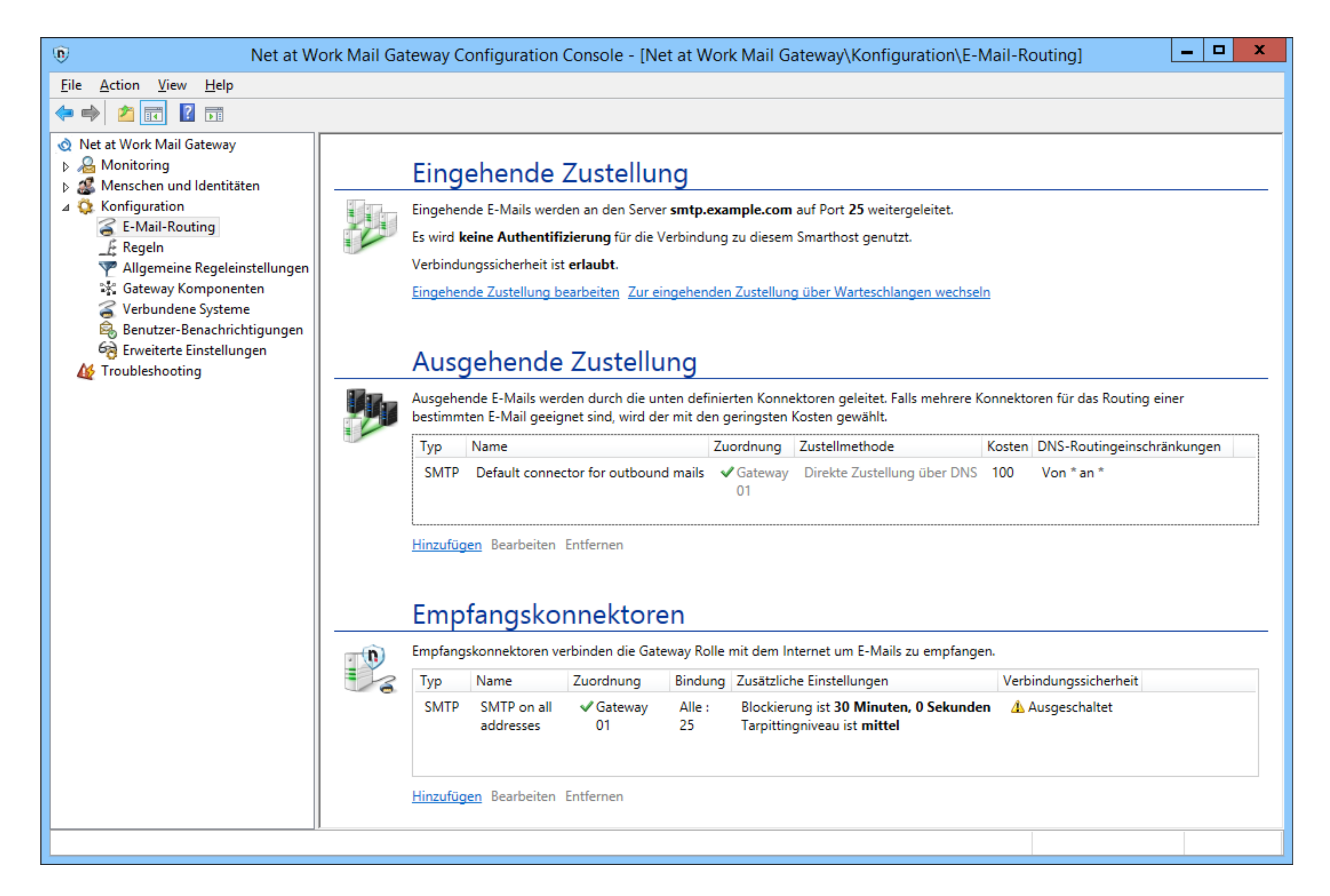


Bild 69: Die Übersicht über alle Konnektoren auf denen das Net at Work Mail Gateway E-Mails empfängt und sendet.

Um die Einstellungen für die Empfangskonnektoren zu ändern, wählen Sie den zu editierenden Empfangskonnektor aus und klicken auf **Empfangskonnektor bearbeiten**.

SMTP Konnektoren

Der SMTP Empfangskonnektor ist die Definition, auf welcher IP-Adresse und welchem Port E-Mails vom Net at Work Mail Gateway empfangen werden. Er legt auch fest, wie mit ungültigen Anfragen von externen E-Mail-Servern verfahren wird und welche Verbindungssicherheit beim Transport der E-Mail angewendet werden soll.

Typ

Wählen Sie in der ersten Seite des Assistenten als **Typ** einen SMTP Konnektor aus.

SMTP Einstellungen

Legen Sie die Gateway-Rollen des Empfangskonnektors fest sowie die IP-Adresse und den Port des Konnektors.

Im Eingabefeld **Bindung auf IP-Adresse** erfolgt die Angabe, unter welcher Adresse die Verbindungen angenommen werden sollen.

Mit der Angabe **Alle** wählen Sie alle vorhandenen IP-Adressen aus. Sie können stattdessen auch eine Auswahl aus der Menge der zugewiesenen IP-Adressen treffen. Klicken Sie hierzu auf das Pfeilsymbol und wählen Sie aus der Auswahlliste die gewünschte IP-Adresse aus.



Wenn Sie mehrere Gateway Rollen ausgewählt haben, dann können Sie keine Bindung auf einzelne IP-Adressen durchführen. Wählen Sie in diesem Fall **Alle** oder **Loopback** aus.

Bei **Port** können Sie den Port einstellen, auf dem das Net at Work Mail Gateway E-Mails empfangen soll.

Ungültige Anfragen

Einige Teilnehmer im Internet versuchen, andere E-Mail-Server durch das Senden von ungültigen Anfragen auszulasten, den sogenannten ‚Denial of Service-Attacken', oder Sicherheitslücken auszunutzen, um in diesen Server einzubrechen. Um diese Angriffe zu minimieren, können Sie solche Anfragen gezielt ausbremsen (z.B. durch sogenanntes „Tarpitting"). Die Karteikarte **Ungültige Anfragen** (Bild 70) zeigt die Konfigurationseinstellungen für diese ungültigen Anfragen.

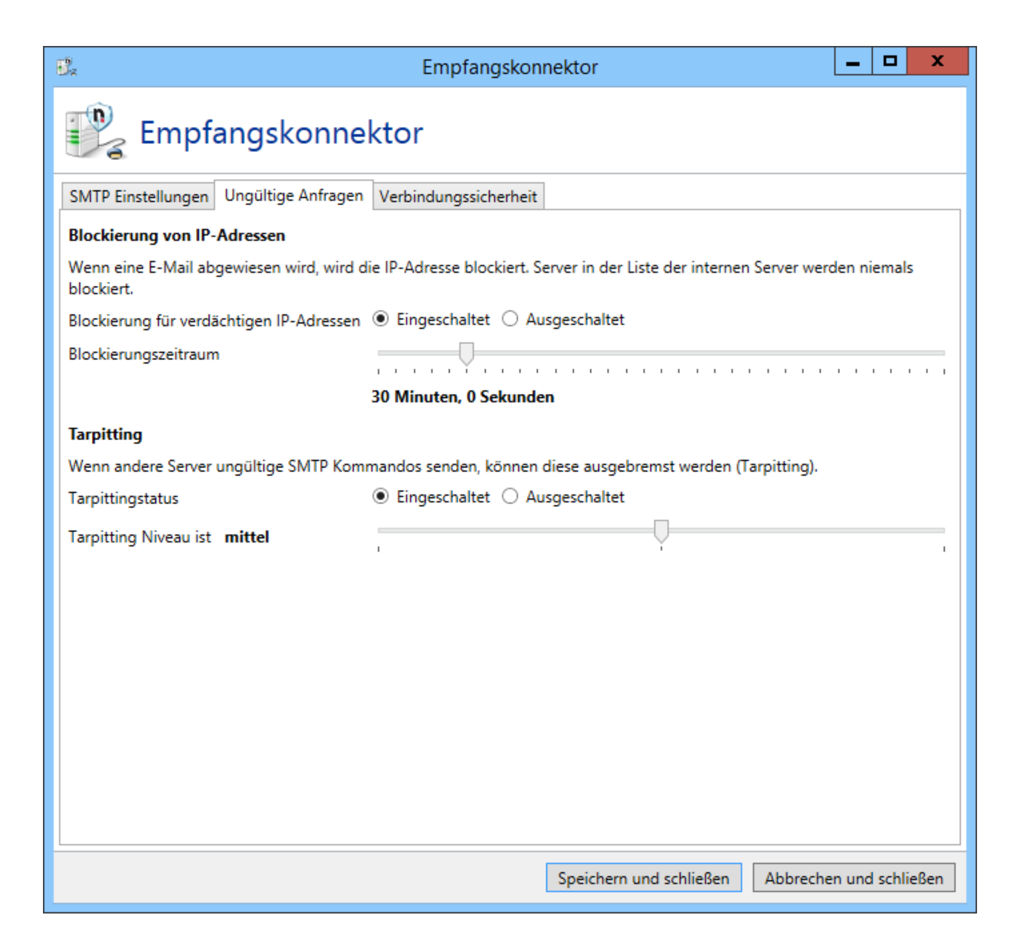


Bild 70: Bestimmen Sie die Verhaltensweise beim Empfang von ungültigen SMTP Kommandos

Die **Blockierung von IP-Adressen** dient dazu, bereits als Spam-Versender erkannte Server gezielt auszubremsen. Wenn ein Server eine E-Mail zu Ihrem Net at Work Mail Gateway sendet und diese als Spam eingestuft wird, werden nachfolgende E-Mails vom gleichen sendenden Server für den angegebenen Zeitraum blockiert. Ein normaler E-Mail-Versender wird nach diesem Zeitraum einen neuen Versuch unternehmen die E-Mail zuzustellen. Ein Spam-Versender wird wahrscheinlich die Zustellung abbrechen und sich auf ungeschützte E-Mail-Empfänger konzentrieren.

Stellen Sie über den Radiobutton **Blockierung für verdächtige IP-Adressen** die Option zur Blockierung ein oder aus. Mit dem Schieberegler für den **Blockierungszeitraum** können Sie die Dauer der Blockierung von 5 Minuten bis zu einem Tag (1440 Minuten) festlegen.

Das „Tarpitting“ ist eine Methode, um Mail-Relays auszubremsen, die sich bei den SMTP-Befehlssätzen und/oder deren korrekte Reihenfolge nicht an die RFC halten. Sobald ein SMTP-Befehl falsch übermittelt oder an der falschen Stelle übermittelt wird, wartet das Net at Work Mail Gateway bei jedem weiteren Befehl 5 Sekunden mit seiner Antwort. Die Übermittlung der Befehle wird also künstlich erschwert, als würden Sie einen Weg durch eine Teergrube nehmen, daher der Name Tarpitting.

Das **Verlangsamen von schlechten Verbindungen erlauben (Tarpitting)** können Sie mit den Radiobuttons **Eingeschaltet** und **Ausgeschaltet** ein- und ausschalten. Mit dem Schieberegler für das **Tarpitting Niveau** können Sie einstellen, um wie viele Sekunden das Net at Work Mail Gateway die

Antwortzeit verzögert. Stellen Sie den Schieberegler auf 'Niedrig', wartet das Gateway 2 Sekunden. In der Einstellung 'Mittel' wartet es 5 Sekunden und in der Position 'Hoch' wartet es 10 Sekunden.

Verbindungssicherheit

Der SMTP Empfangskonnektor nutzt in der Verbindungssicherheit eine Server-Identität.

Wenn Sie StartTLS oder SMTPS als Verbindungssicherheit verlangen, können Sie zusätzlich auch die Identität des einliefernden Servers sicherstellen (Bild 71). Dabei sind folgenden Einstellungen möglich:

- **Erlaube Verbindungen von jedem Server**
  Die Identität des einliefernden Servers wird hier nicht beschränkt. Es werden E-Mails von allen Servern angenommen.
- **Verlange ein Zertifikat**
  Das hier auszuwählende Zertifikat kann sowohl ein Endzertifikat als auch ein Zwischen- oder Stammzertifikat sein. Wenn Sie ein Endzertifikat auswählen, muss der einliefernde Server seine Identität mit diesem belegen. Wenn Sie ein Zwischen- oder Stammzertifikat auswählen muss er seine Identität mit einem Zertifikat belegen, dass das angegebene Zertifikat als Zwischen- oder Stammzertifikat in seiner Zertifikatskette besitzt.
- **Verlange ein vertrautes Zertifikat**
  Der einliefernde Server muss seine Identität mit einem Zertifikat belegen, das im Zertifikatsspeicher des lokalen Computers als vertrauenswürdig hinterlegt ist.

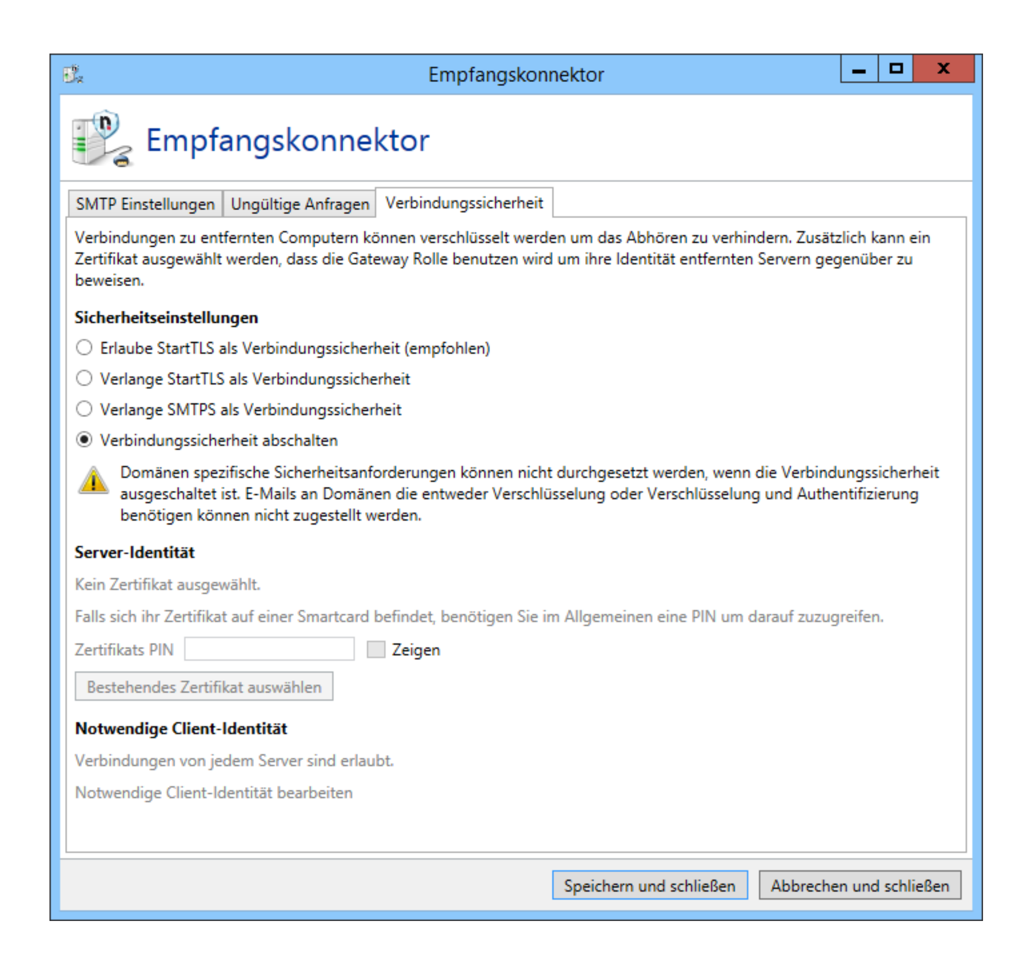


Bild 71: Anzeige der notwendigen Client-Identität in der Verbindungssicherheit des SMTP Empfangskonnektors

De-Mail-Konnektor

Wählen Sie in der ersten Seite des Dialogs **Neuer Empfangskonnektor** Ihren De-Mail-Dienstanbieter aus. (Bild 72).

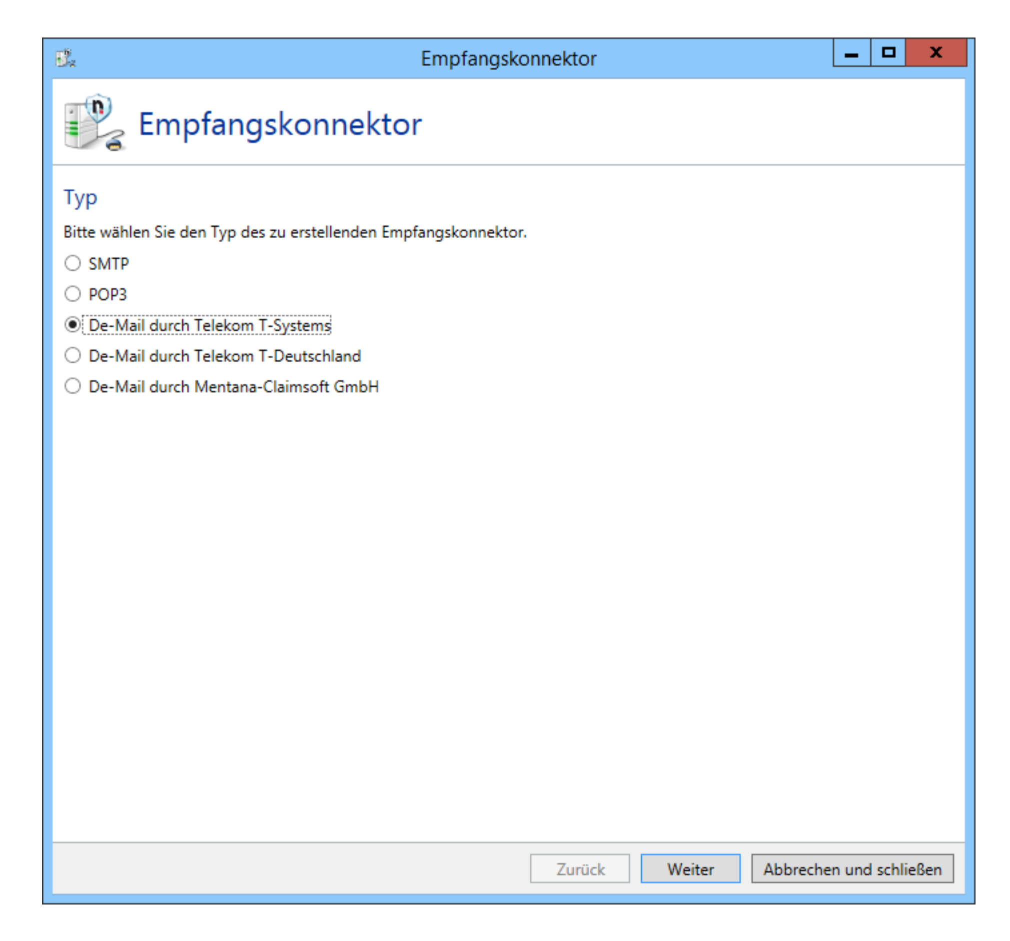


Bild 72: Die Auswahl des Konnektortyps

Legen Sie für zuerst einen Namen und den oder die Gateway-Rollen fest. Bestimmen Sie durch die Einstellung des **Herunterladeintervalls** wie oft das Net at Work Mail Gateway das De-Mail-Postfach auf neue Nachrichten überprüfen soll. Nun können Sie den Anbieter wählen und konfigurieren.

Mentana-Claimsoft GmbH Anbieter

Für die Anbindung an Mentana Claimsoft ist noch ein weiterer Konfigurationsschritt notwendig. Sobald die Verbindung zum Webservice Proxy konfiguriert ist, lädt der Empfangskonnektor die Liste aller zur Verfügung stehenden Mailbox-Namen. Jede dieser Mailboxen benötigt eine Rückfalladresse. Diese wird für die Zustellung genutzt, falls der ursprüngliche Empfänger der E-Mail in Ihrem Unternehmen nicht mehr verfügbar ist. Sobald für alle Mailboxen Rückfalladressen konfiguriert sind, ist die Konfiguration des Mentana-Claimsoft Empfangskonnektors vollständig.

De-Mail-Anbieter 'T-Deutschland' und 'T-Systems'

Bei dem De-Mail-Konnektor für T-Systems oder T-Deutschland sind noch zwei Einstellungen notwendig. (Bild 73). Legen Sie eine **interne Rückfalladresse für eingehende E-Mails** fest. Diese wird für die Zustellung genutzt, falls der ursprüngliche Empfänger der E-Mail in Ihrem Unternehmen nicht mehr verfügbar ist. Außerdem können Sie hier wählen, ob De-Mails vom Server des Dienstanbieters gelöscht werden oder dort gespeichert bleiben.



Bild 73: Die Konfiguration eines Telekom De-Mail-Anbieters

Im Dialog für die Verbindungsicherheit wählen Sie bitte das für die Verbindung notwendige Zertifikat aus. (Bild 74)

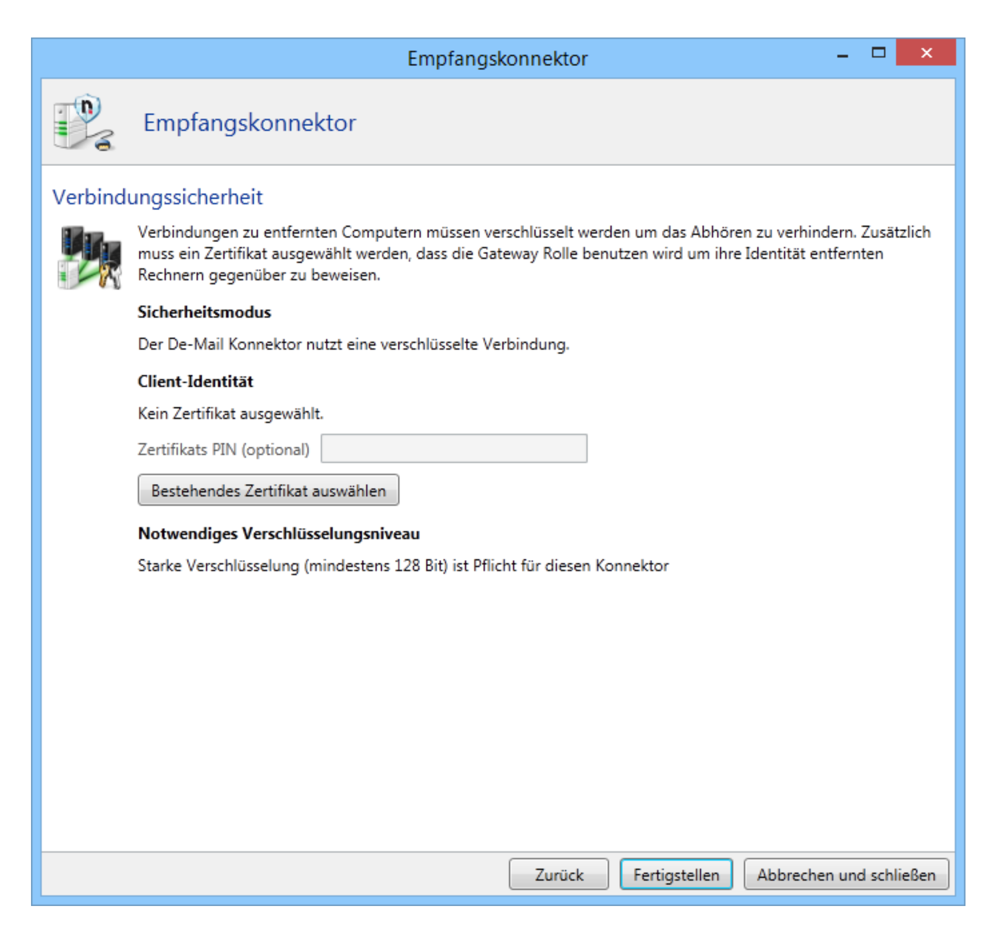


Bild 74: Die Verbindungssicherheit eines Telekom oder T-Systems De-Mail-Empfangskonnektors

POP3 Konnektor

Mit dem POP3 Konnektor können externe POP3 Postfächer durch das Net at Work Mail Gateway auf neue E-Mails überprüft und abgeholt werden. Alle abgeholten E-Mails werden dann vom Gateway an die konfigurierte interne Adresse zugestellt.

Typ

Wählen Sie in der ersten Seite des Assistenten als **Typ** einen POP3 Konnektor aus.

POP3 Empfangskonnektor

Neben den allgemeinen Einstellungen, wie Name und Anbindung an Gateway Rollen geben Sie hier zunächst die Benutzerinformationen für den Zugriff auf das POP3-Konto an.

Das Abholintervall bestimmt, wie oft das POP3 Postfach auf neue E-Mails kontrolliert wird.

Im Bereich **E-Mail-Zustellung** wird neben einer internen E-Mail-Adresse auch das Zustellverhalten konfiguriert. Wenn Sie als Zustelloption **Alle E-Mails an die zugeordnete interne E-Mail-Adresse zustellen** ausgewählt haben, werden die Empfängerdaten in den abgeholten E-Mails ignoriert und die E-Mails werden alle an die angegebene Adresse gesendet. Bei Auswahl der zweiten Option

werden die Empfängerdaten aus den eingehenden E-Mails extrahiert und die E-Mails werden an die entsprechenden Empfänger weitergeleitet. Die angebene Adresse wird nur für E-Mails verwendet, in denen keine internen E-Mail-Adressen gefunden werden kann.

Sie können hier außerdem festlegen, ob die E-Mails nach dem Herunterladen vom Server entfernt werden. Falls Sie die E-Mails auf dem Server lassen, dann werden sie trotzdem nur einmalig heruntergeladen.

Verbindungssicherheit

Der Empfangskonnektor nutzt in der Verbindungssicherheit eine Server-Identität. Als Sicherheitseinstellungen für die Verbindungssicherheit stehen hier die Optionen TLS als Verbindungssicherheit nutzen, für eine Verbindung zu einem Server der eine verschlüsselte Verbindung über POP3S unterstützt, und Verbindungssicherheit abschalten für eine unverschlüsselte Verbindung über POP3 zur Verfügung.

Regeln

Um eine E-Mail zu bearbeiten, wendet das Net at Work Mail Gateway Regeln an, die Sie individuell konfigurieren können.

Nach der Neuinstallation des Net at Work Mail Gateways kann nach dem Einspielen der Lizenz ein Satz von Standardregeln erstellt werden. Diese helfen Ihnen, dass das Gateway möglichst schnell und mit minimalem Administrationsaufwand die Funktion aufnehmen kann. Trotzdem sollten Sie diese Regeln überprüfen und ggf. an Ihre Bedürfnisse anpassen.

Die Regeln des Net at Work Mail Gateways sind modular aufgebaut. Sie können selbst Regeln erstellen und bereits bestehende Regeln ändern. Dies tun Sie, in dem Sie für jede einzelne Regel aus den zur Verfügung stehenden Filtern die gewünschten Filter auswählen. Innerhalb jeder Regel können Sie diese beliebig gewichten und ggf. konfigurieren.

Die Filter übernehmen bei der Prüfung der E-Mail die eigentliche Arbeit, sie bewerten, wie stark die E-Mail ein bestimmtes Filterkriterium erfüllt und vergeben dafür Punkte. Wie diese Punkteverteilung genau vor sich geht, wird weiter unten erläutert. Sie können also Ihr eigenes Regelwerk mit ganz verschiedenen Filterkombinationen aufstellen und die Regeln auf bestimmte Sender und Empfänger einschränken. Das hat mehrere Vorteile, denn so können Sie sehr individuell und flexibel auf Spam-Attacken reagieren. Nicht jede verdächtige E-Mail ist in jeder Situation für jedes Unternehmen Spam.

Wenn Sie z. B. einen Wortfilter einsetzen, ist der Ausdruck „Viagra“ sehr wahrscheinlich auf Ihrer „schwarzen“ Liste; Sie möchten E-Mails mit „Viagra“-Werbung blocken. Für ein Pharma-Unternehmen ist dieser Ausdruck jedoch nur sehr bedingt ein Spam-Kriterium. Mit NoSpamProxy können Sie selbst aussuchen, ob Sie „Viagra“ in den Wortfilter aufnehmen; oder ob Sie überhaupt einen Wortfilter einsetzen und wenn ja, wie stark Sie ihn gewichten.

Wenn eine E-Mail ansonsten seriös erscheint oder von einem bekannten E-Mail-Sender kommt, kann das Auftreten des verdächtigen Wortes unter Umständen akzeptabel sein. Sie können auch festlegen, dass die Regel mit dem Wortfilter nur für bestimmte IP-Adressen oder Empfänger gilt; zum Beispiel nur für Absender mit einer bestimmten TLD (Top Level Domain) oder IP-Adressen aus einem bestimmten Subnetz.

Die Reihenfolge der Regeln ist wichtig. Wenn eine Regel für eine zu überprüfende E-Mail zuständig ist, wird sie genutzt. Falls mehrere Regeln für eine E-Mail zutreffen, kommt diejenige Regel zur Anwendung, die in der Liste am weitesten oben steht.

Pos.	Regelname	Von	An	Aktion
1	"Allgemein"	*	max.mustermann@example.com	
2	"Japan"	*.jp	max.mustermann@example.com	

Regel 1, die wir hier „Allgemein“ nennen, ist definiert auf alle E-Mails, die an max.mustermann@example.com adressiert sind. Regel 2 mit dem Namen "Japan" auf Position 2 ist ebenfalls auf Empfänger max.mustermann@example.com definiert, berücksichtigt aber nur Absender aus Japan.

Auf eine E-Mail aus Japan an „max.mustermann“ treffen beide Regeln zu. Doch nur die Regel "Allgemein" wird zur Bewertung herangezogen, weil sie in der Liste oben steht. Auch wenn die Japan-Regel eigentlich „genauer“ wäre - die Reihenfolge ist das entscheidende Kriterium.

Pos.	Regelname	Von	An	Aktion
1	"Japan"	*.jp	max.mustermann@example.com	
2	"Allgemein"	*	max.mustermann@example.com	

Filter

Für jede E-Mail werden die einzelnen Filter der zutreffenden Regel ausgeführt. Die Filter bewerten und vergeben Malus- und Bonus-Punkte für die zu überprüfende E-Mail. Diese Punkte werden, entsprechend der Gewichtung der einzelnen Filter, zu einem Gesamtwert addiert. Überschreitet dieser Wert den eingestellten Schwellenwert (SCL) der Regel, wird die E-Mail abgewiesen. Den Schwellenwert können Sie individuell für jede Regel einstellen.

Welche Filter zur Verfügung stehen und wie sie genau funktionieren, erfahren Sie in Kapitel Filter im Net at Work Mail Gateway.

Aktionen

Aktionen bei der Spam-Prüfung

Nachdem anhand der Filter bestimmt wurde, ob die E-Mail abgewiesen wird oder passieren darf, werden die konfigurierten Aktionen aufgerufen. Aktionen können unter anderem die E-Mails verändern, um z. B. eine Fußzeile zu ergänzen oder unerwünschte Anlagen zu entfernen. Aktionen können aber auch E-Mails, die nach der Bewertung durch die Filter eigentlich passieren würden, trotzdem abweisen. Damit kann beispielsweise ein Virenscanner die E-Mail noch abweisen, obwohl sie nicht als Spam erkannt wurde.

Dies bedeutet, dass Aktionen übergeordnete Einstellungen sind, mit denen Filter gegebenenfalls überstimmt werden können.

Alle Aktionen werden im Kapitel Aktionen im Net at Work Mail Gateway detailliert beschrieben.

Wie NoSpamProxy eine E-Mail als Spam klassifiziert

In den Regeln können Sie verschiedene Filter und Aktionen konfigurieren. Die Filter innerhalb einer Regel sind die Prüfstellen, welche nach bestimmten Kriterien den Spam-Charakter einer E-Mail bewerten. Je höher die Spamwahrscheinlichkeit ist, desto höher wird das Punktergebnis für diese E-Mail. Wird eine E-Mail hingegen als eher vertrauenswürdig bewertet, dann kann das Ergebnis auch negativ werden. Der Wertebereich liegt zwischen -10 und +10 Punkten. Die Filter können Sie innerhalb der Regeln verschieden gewichten. Je nach Gewichtung wird die Bewertung des Filters dann vervielfacht. Auf diese Art und Weise können Sie den Einfluss (=Punktbeitrag) eines wichtigen Filters innerhalb einer Regel erhöhen.

Anhand der ermittelten Gesamtpunktzahl wird ein „Spam Confidence Level“ (SCL) ermittelt. Ein SCL von 0 besagt, dass die E-Mail neutral eingestuft wurde. Je größer der Wert ist, desto mehr wurde die E-Mail als Spam klassifiziert. Ist der Wert kleiner 0, dann wurde die E-Mail als vertrauenswürdig eingestuft. Erreicht diese Gesamtgewichtung den Schwellenwert der Regel, wird die E-Mail als Spam behandelt und abgewiesen.

Nehmen wir zur Veranschaulichung folgendes Beispiel:

Sie haben eine Regel erstellt mit einem aktiven Filter: Dem Wortfilter. Außerdem ist das Level-of-Trust-System für diese Regel aktiviert. Der Wortfilter überprüft eine E-Mail auf unerwünschte Ausdrücke.

Nehmen wir ferner an, eine eingehende E-Mail enthält eine Vielzahl von unerwünschten Ausdrücken. Der Wortfilter wird daher bei dieser E-Mail Alarm schlagen und einen hohen Malus-Wert liefern, zum Beispiel **6**. Wäre der Wortfilter der einzige Filter in dieser Regel, würde die E-Mail nun einen Gesamtwert von **6** haben. Wenn Sie in der Regel beispielsweise den Schwellenwert mit der Zahl **4** eingestellt haben, würde die E-Mail jetzt geblockt und abgewiesen werden. Der Absender würde eine Unzustellbarkeitsnachricht erhalten.

Nun ist in dieser Regel noch das Level-of-Trust-System aktiviert. Die E-Mail kommt von einem sehr verlässlichen Mailpartner, mit dem Sie bereits viele E-Mails ausgetauscht haben. Das Level-of-Trust-System bewertet diese E-Mail mit **-4** SCL-Punkten. Das Level-of-Trust-System hat immer eine Gewichtung, die der Summe der Gewichtungen aller auf der Regel aktivierten Filter plus **1** entspricht. Dies ergibt einen Faktor von **2** in unserem Beispiel. Der SCL Wert ergibt sich also aus **6+2*-4**. Damit ergibt sich ein SCL von **-2**. Die E-Mail würde NoSpamProxy passieren.

Schon bei diesem kleinen Beispiel deutet sich an, welche Möglichkeiten der modulare Aufbau der Regeln bietet und wie wichtig die Filtergewichtung sein kann. SCL-Berechnungen werden im Kapitel Berechnung des Spam Confidence Levels detailliert beschrieben.

Ein weiteres aufschlussreiches Beispiel ist der folgende Fall:

Eine E-Mail kommt von einem System, das auf einer Sperrliste (RBL) steht. Die meisten Filterprodukte würden eine solche Verbindung ohne nähere Analyse kategorisch ablehnen. Mit NoSpamProxy jedoch können Sie diese Entscheidung relativieren. Wenn die E-Mail z. B. eine Antwort darstellt, dann kann der

Level-of-Trust-Filter die Bewertung überstimmen. Ergebnis: Die E-Mail von diesem Absender wird nicht geblockt, sondern, wie erwünscht, zugestellt.

E-Mails von einem anderen unbekannten Absender, der diesen unsicheren Server missbraucht, können aber nicht passieren.

Konfiguration der Regeln

Die Regeln, wie E-Mails bearbeitet werden sollen, werden im Knoten **Regeln** gepflegt (Bild 75).

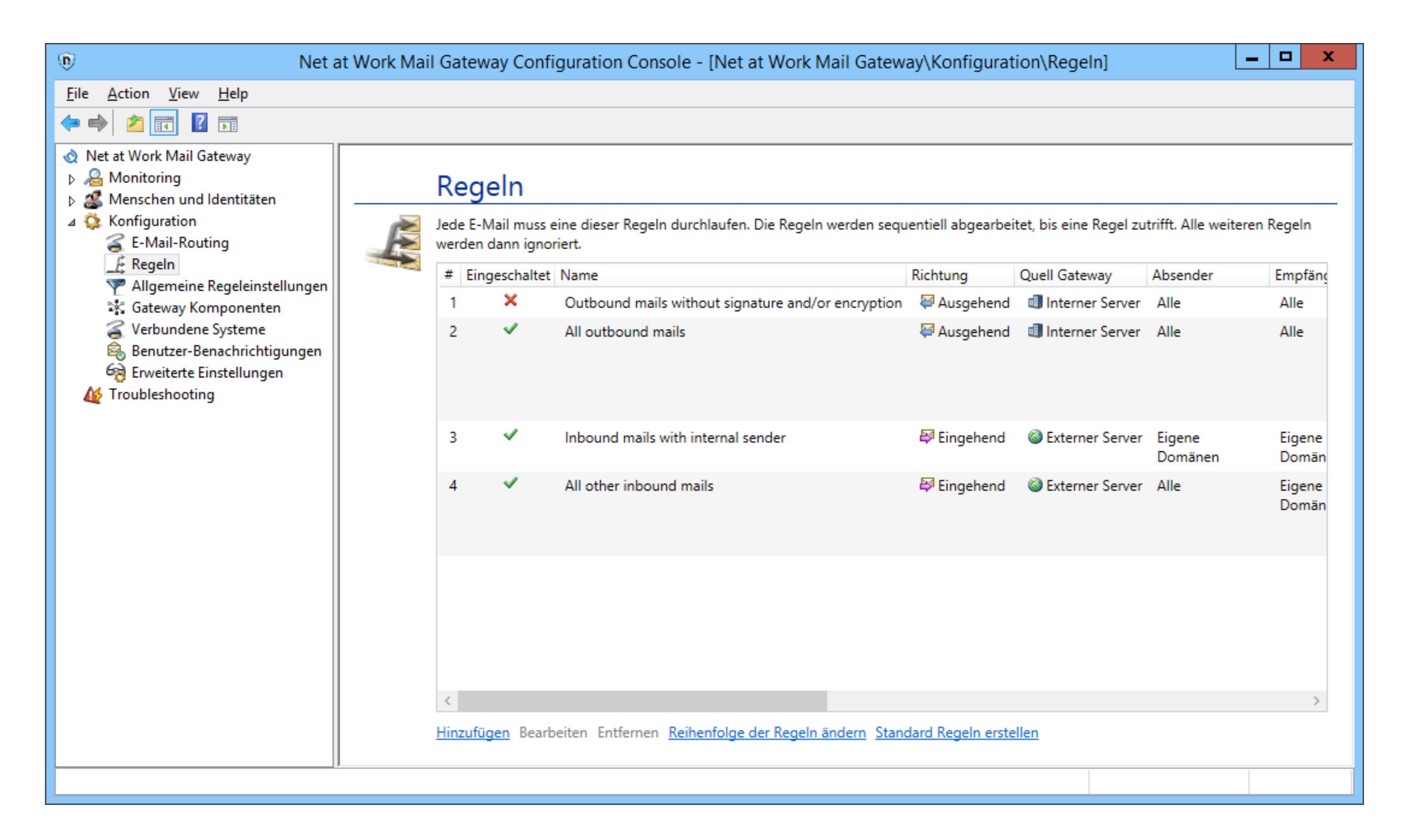


Bild 75: Die Übersicht über alle Regeln, die die Verarbeitung der E-Mails bestimmen

Bei einer Neuinstallation des Net at Work Mail Gateways ist die Auflistung der Regeln leer. In diesem Fall können Sie die Standard Regeln erzeugen lassen, in dem Sie den Link **Standard Regeln erstellen** nutzen (Bild 76). Die Funktion für die Erzeugung von Standard Regeln steht Ihnen auch später zur Verfügung, falls Sie Ihre eigenen Regeln mit den Standard Regeln ergänzen oder ersetzen möchten. Beim Ergänzen werden die Standard Regeln hinter die bestehenden Regeln angefügt und können danach in der Reihenfolge verändert werden, siehe Reihenfolge der Regeln ändern.



Bild 76: Lassen Sie sich die Standard Regeln automatisch erstellen

Neue Regel erstellen

Eine Regel besitzt folgende Einstellungen: **Allgemein**, **Richtlinienverstoß**, **Gateways**, **Absender**, **Empfänger**, **Filter** und **Aktionen**. Welche Regel für eine E-Mail zur Anwendung kommt, wird durch die Einstellungen der Reiter **Gateways**, **Absender** und **Empfänger** festgelegt. Die anderen Reiter legen fest, wie die E-Mails verarbeitet werden.

Der erste Reiter (Bild 77) umfasst wichtige Parameter mit denen Sie grundlegende Eigenschaften festlegen.

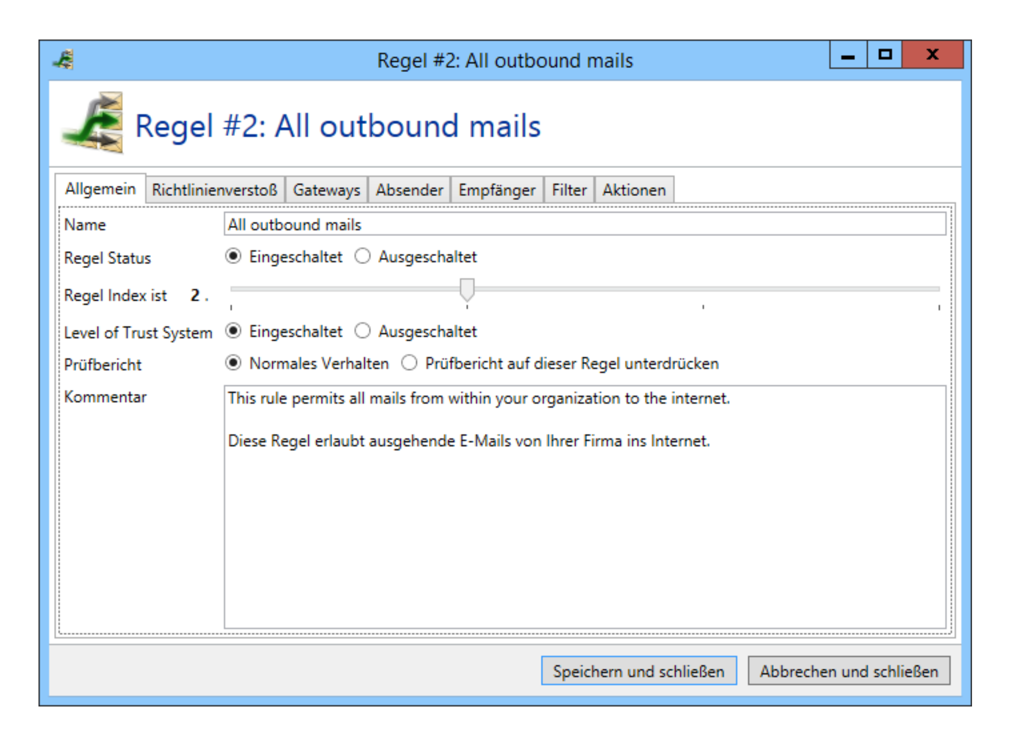


Bild 77: Allgemeine Einstellungen der Regel

Zunächst geben Sie einen eindeutigen Namen für die Regel an, damit Sie in der Regelzusammenfassung nicht den Überblick verlieren. Unter **Aktiv** können Sie angeben, ob die Regel aktiviert oder deaktiviert ist. Mit dem **Index** der Regel geben Sie die Rangfolge der entsprechenden Regel ein.

Mit der Option **Level-of-Trust-System** können Sie das Level-of-Trust-System auf der Regel ein- oder abschalten.

Unter **Anmerkungen** können Sie eine Anmerkung zu der Regel festhalten, um die Identifizierung der Regel zu erleichtern. Die Anmerkungen haben keine Auswirkung auf Definition oder Funktion einer Regel. Sie dienen nur der Dokumentation.

Auf dem zweiten Reiter können Sie Einstellungen zum **Richtlinienvertoß** konfigurieren. Falls eine E-Mail die von Ihnen eingestellten Richtlinien für den Versand oder Empfang nicht erfüllt, wird das hier konfigurierte Verhalten verwendet. Richtlinienverstöße entstehen z.B. wenn eine E-Mail nicht verschlüsselt werden konnte oder weil ungültige Anhänge in E-Mails gefunden wurden.

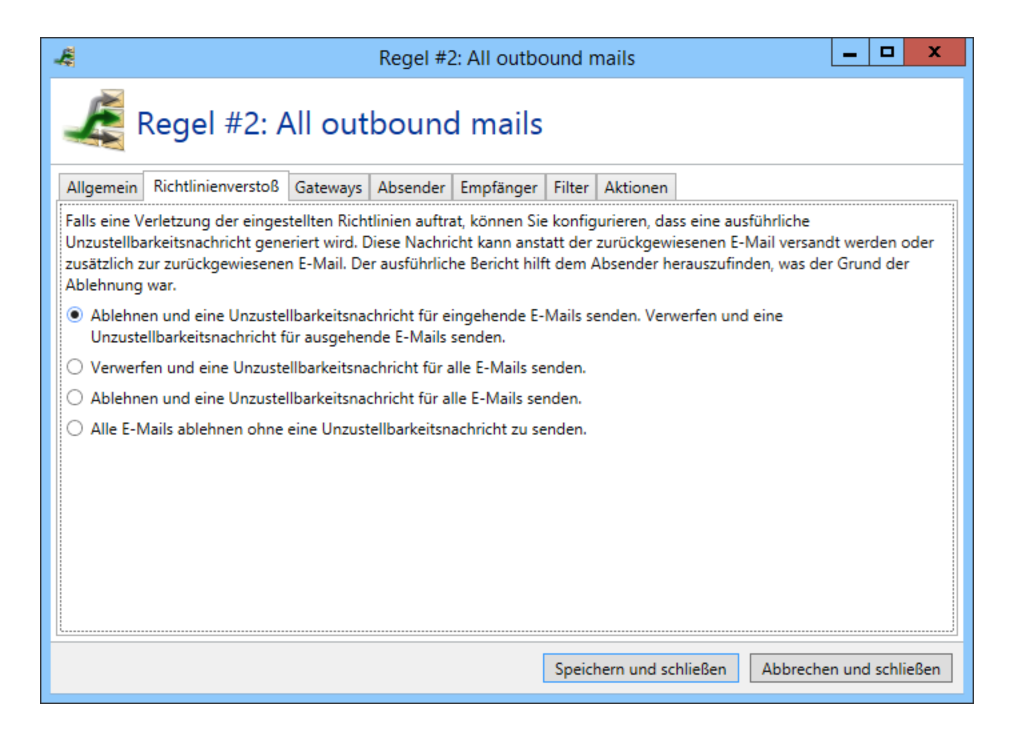


Bild 78: Verhalten bei Richtlinienverstoß

Ihnen stehen folgende Optionen zur Verfügung. **Ablehnen** einer E-Mail bedeutet, dass der empfangende Server die Annahme verweigert (SMTP-Meldung 5xx). Dadurch muss der einliefernde Server eine Unzustellbarkeitsnachricht (NDR) generieren. **Verwerfen** bedeutet eine positive Quittierung des empfangenden Servers an den einliefernden Server (SMTP-Meldung 200) aber ohne weitere Verarbeitung der empfangenen E-Mail. Da die E-Mail direkt nach der Annahme gelöscht wird, wird das Net at Work Mail Gateway eine Unzustellbarkeitsnachricht generieren und an den einliefernden Server zurücksenden.

Im **Gateway** Reiter (Bild 79) geben Sie an, für welches Gateway die Regel gelten soll, bezogen auf Extern/Intern und die IP-Adresse. Dadurch kann in diesem Reiter auf den Namen oder die IP-Adresse des sendenden Mail Servers gefiltert werden.

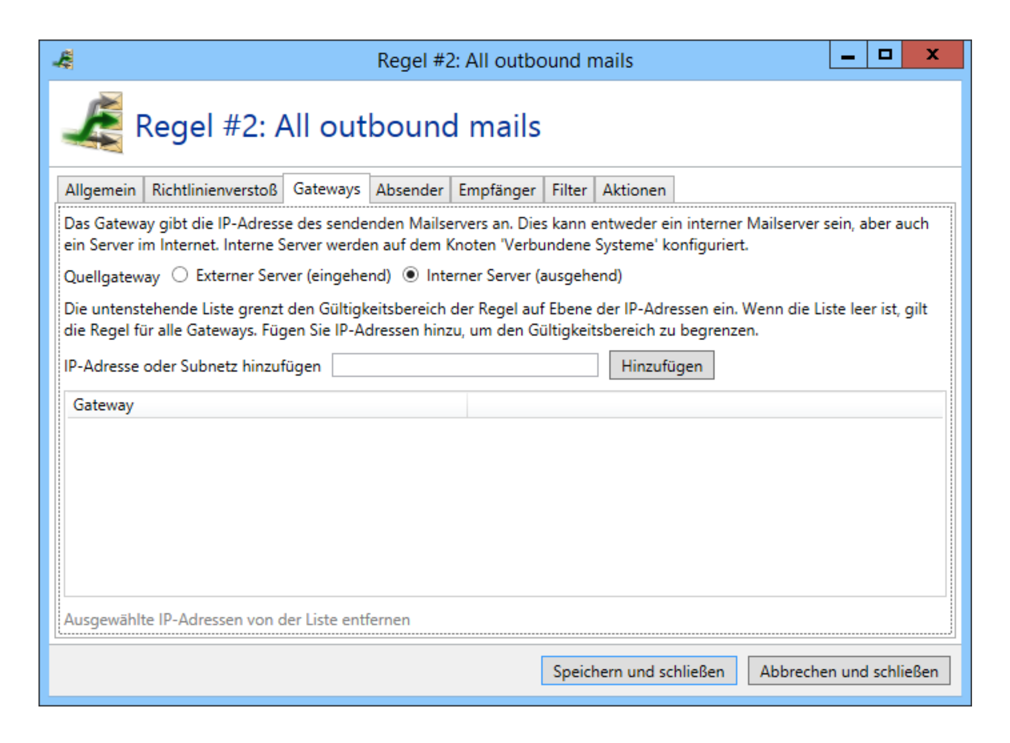


Bild 79: Definieren Sie die Gültigkeit der Regel in Bezug auf den sendenden Mail-Server

Unter **Quellgateway** klicken Sie **Externer Absender** für eingehende E-Mails oder **Interner Absender** für ausgehende E-Mails an. Das Net at Work Mail Gateway erkennt anhand der Liste der internen E-Mail-Server, ob eine E-Mail von außen nach innen oder von innen nach außen übertragen wird.

Wenn hinsichtlich des Gateways keine Filterung vorgenommen werden soll, lassen Sie den Bereich **Gateway** leer. Das bedeutet, dass diese Regel alle IP-Adressen einbezieht. Alternativ können Sie hier ein bestimmtes Subnetz oder eine konkrete IP-Adresse angeben.

Auch den **Absender** können Sie über den entsprechenden Reiter nach Kategorie und spezifischer Adresse einschränken (Bild 80)

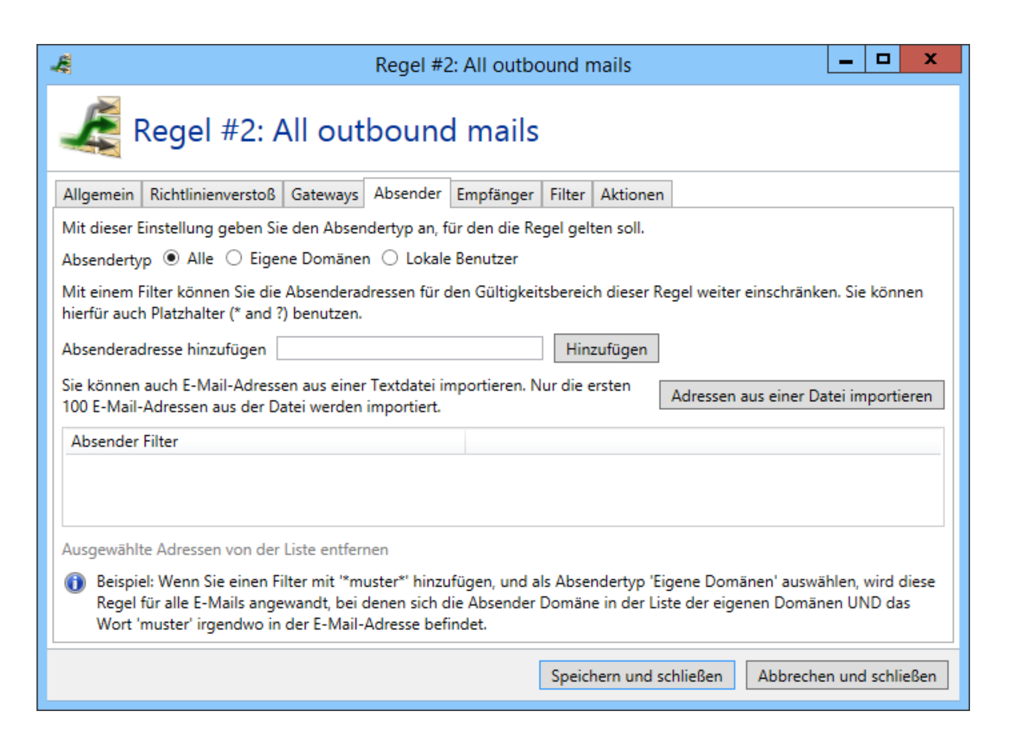


Bild 80: Geben Sie den Absender der E-Mail für diese Regel an

Unter **Absendertyp** wählen Sie zunächst den Typ **Alle**, **Lokale Domänen** oder **Lokale Adressen**, für den die Filter-Einstellung gelten soll. Im Bereich **Absender Filter** nehmen Sie keine Änderungen vor, wenn alle Absender in die Auswahl kommen sollen. Alternativ können Sie eine benutzerdefinierte Auswahl treffen, in dem Sie hier die entsprechenden E-Mail-Adressen hinzufügen. Sie können auch mit Platzhaltern ('*' und '?') arbeiten.

Um die E-Mail-Adressen nicht alle manuell angeben zu müssen, können Sie die Import-Funktion nutzen, um das Feld **Absender Filter** zu füllen. Klicken Sie dazu auf **Adressen aus einer Datei importieren**.

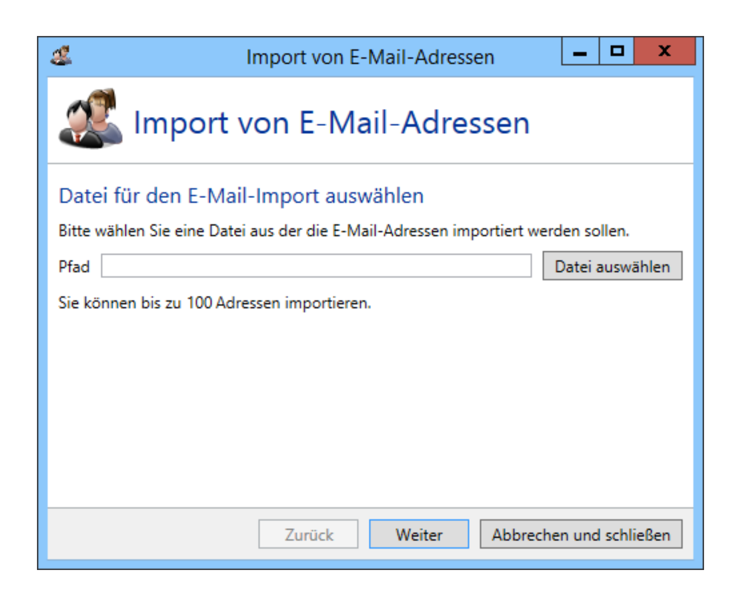


Bild 81: Importieren Sie E-Mail-Adressen aus einer Textdatei

Klicken Sie in dem Dialog **Import von E-Mail-Adressen** (Bild 81) auf **Datei auswählen** und geben Sie dort dann den Pfad und den Namen der zu importierenden Datei an und klicken anschließend auf **Weiter**.

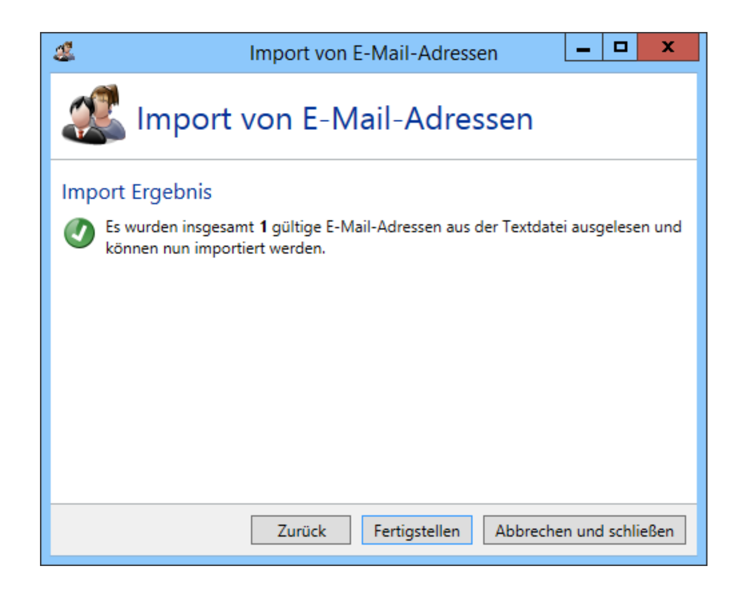


Bild 82: Der Assistent extrahiert alle gültigen E-Mail-Adressen aus der Datei

Im abschließenden Dialog (Bild 82) wird das Ergebnis des Imports angezeigt.



Es werden lediglich bis zu 100 Adressen importiert. Wenn Sie weitere Adressen hinzufügen möchten, müssen Sie den Vorgang mit einer zweiten Datei wiederholen. Mehr als 100 Adressen in einer Regel zu pflegen, ist aus Performancegründen nicht empfohlen.

Ähnlich zum Reiter **Absender** können Sie im Reiter **Empfänger** Adressen definieren, die eine E-Mail besitzen muss, damit diese Regel angewandt wird (Bild 83).

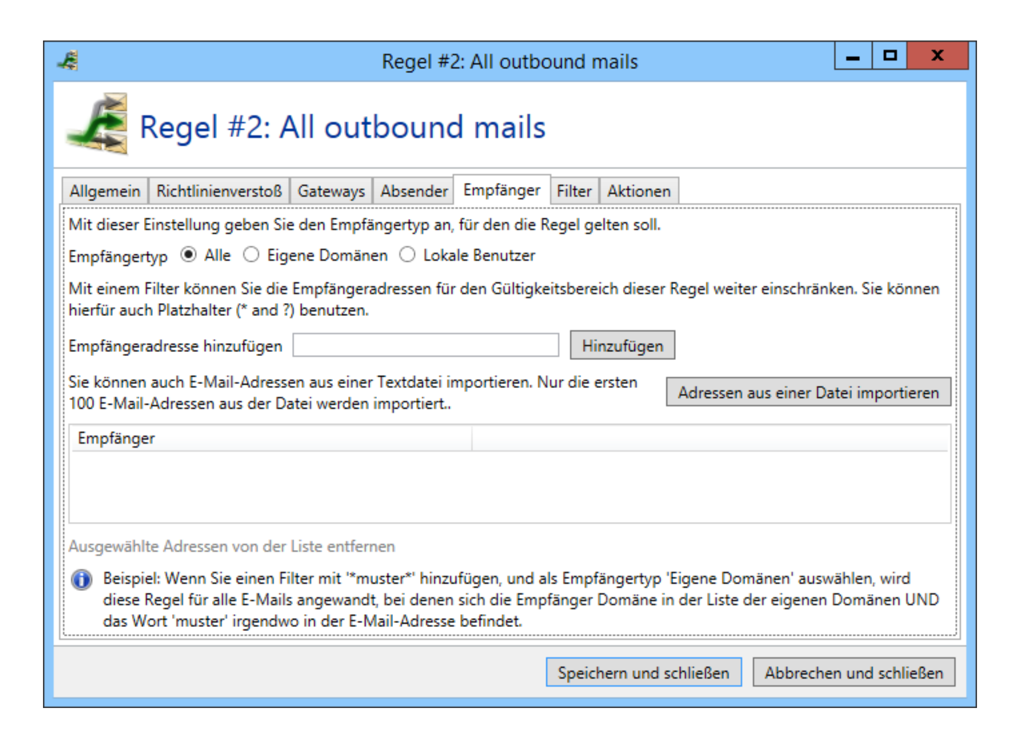


Bild 83: Definieren Sie die Empfänger einer E-Mail bei denen diese Regel zutrifft

Unter **Empfängertyp** wählen Sie wiederum zunächst den Typ **Alle**, **Lokale Domänen** oder **Lokale Benutzer**. Im Bereich **Empfänger Filter** nehmen Sie keine Änderungen vor, wenn alle Empfänger in die Auswahl kommen sollen.

Alternativ können Sie eine benutzerdefinierte Auswahl treffen, in dem Sie hier die entsprechenden E-Mail-Adressen hinzufügen.

Auch Empfänger können über einen Importvorgang, wie in der Registerkarte **Absender**, über eine Textdatei hinzugefügt werden.

Im Reiter **Filter** aktivieren Sie die gewünschten Filter für eine Regel (Bild 84). Die Filter wiederum können Sie unterschiedlich gewichten und so ihre Wirkung erhöhen oder verringern.

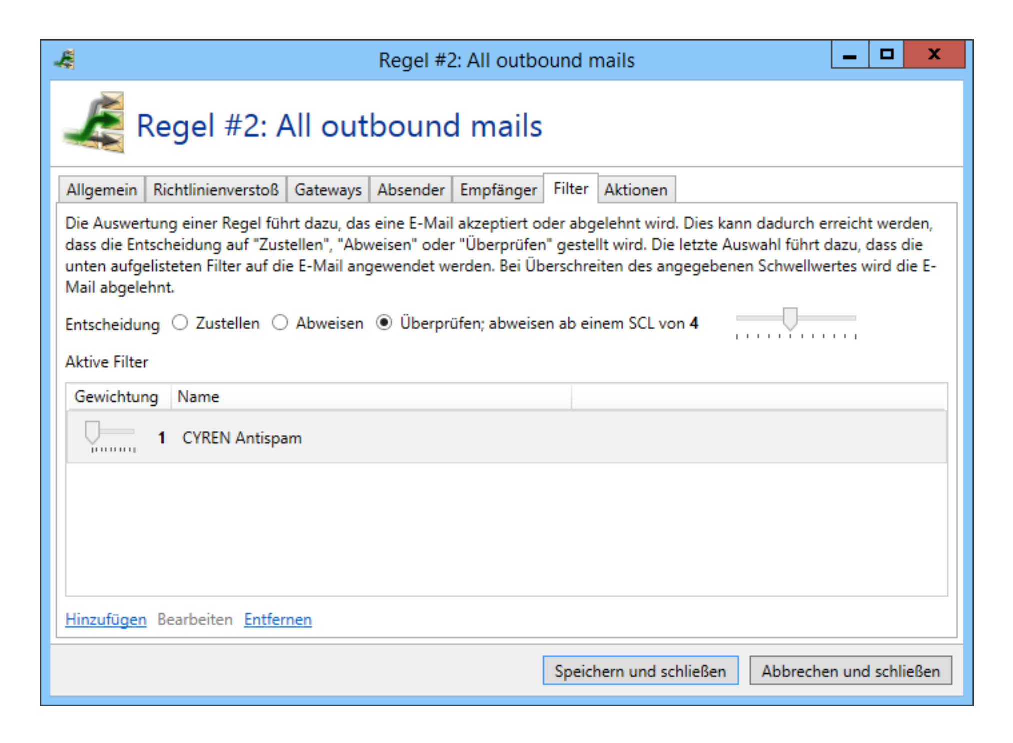


Bild 84: Legen Sie die Filtereinstellungen der Regel fest

Stellen Sie die **Filtereinstellung** auf **Abweisen**, wenn alle E-Mails, die von dieser Regel verarbeitet werden, ungeprüft abgewiesen werden sollen. Wählen Sie **Zustellen**, wenn alle E-Mails dieser Regel ungeprüft zugestellt werden sollen. Mit **Überprüfen** wird das Spam Confidence Level (SCL) jeder E-Mail überprüft und beim Erreichen des eingestellten Wertes als Spam abgewiesen. Ein SCL-Wert von „1“ bedeutet, dass E-Mails bei geringen Spam Anzeichen bereits abgewiesen werden. Ein SCL-Wert von „10“ weist nur E-Mails mit extrem hohen Spam Anzeichen ab.

Nur wenn Sie die Filtermethode **Überprüfen** ausgewählt haben, können Sie diejenigen Filter auswählen, die Sie einsetzen möchten. Hierzu dient der Bereich **Aktive Filter**. Um einen oder mehrere Filter für eine Regel zu aktivieren, klicken Sie auf den Link Filter hinzufügen. Es öffnet sich ein Dialog, in dem Sie aus den verfügbaren Filtern den gewünschten Filter auswählen können (Bild 85). Je nach Filter öffnet sich nochmal ein filterspezifischer Konfigurationsdialog, in dem Sie die Filterkonfiguration vornehmen. Links neben den Filternamen finden Sie jeweils einen Regler, mit dem Sie die Gewichtung einstellen können. Der Wert „5“ bedeutet, dass der Filter fünfmal stärker gewichtet wird als ein Filter mit dem Wert „1“.

Einige Filter sind nicht für die in der Regel gewählte Richtung funktionsfähig. Dort wird in der Spalte **Status** der Text **Kann nicht auf eingehenden (bzw. ausgehenden) Regeln angewandt werden**. Solche Filter können nicht hinzugefügt werden und eine Regel mit ungültigen Filtern wird auch nicht abgespeichert.



Das Hinzufügen eines Filters an eine Regel aufgrund der Richtung wird nur verhindert, falls er für diese Richtung keine Funktion zeigt. Diese Beschränkung stellt nicht immer den empfohlenen Einsatz dar. Das heißt, dass Filter die für eine bestimmte Richtung gedacht sind, aber auch in der Gegenrichtung funktionieren, somit für beide Richtungen konfigurierbar sind. Die empfohlene Richtung steht dagegen teilweise im Namen des Filters.

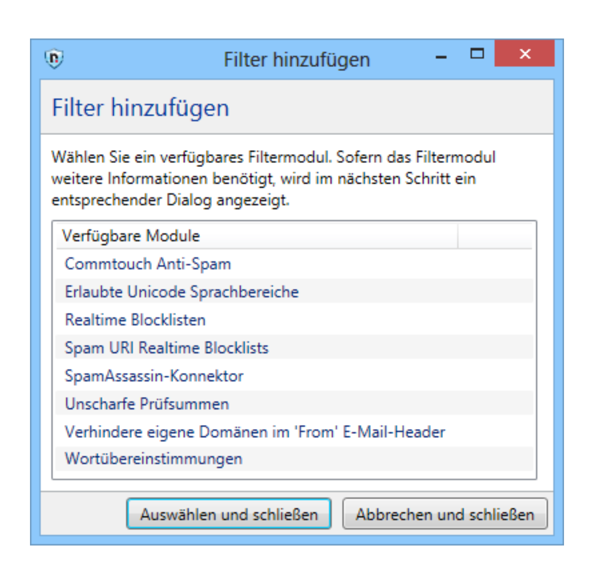


Bild 85: Fügen Sie einen verfügbaren Filter zu Ihrer Regel hinzu

Aktionen werden auf jeder geprüft oder ungeprüft zugestellten E-Mail ausgeführt. Sie können in diesem Reiter entscheiden welche Aktionen in der Regel ausgeführt werden und wie diese Aktionen in der Regel konfiguriert werden. Aktionen werden immer ausgeführt, auch wenn die E-Mails nicht durch Filter überprüft werden.

Die in der Regel aktiven Aktionen werden in der Liste **Aktive Aktionen** aufgeführt (Bild 86).

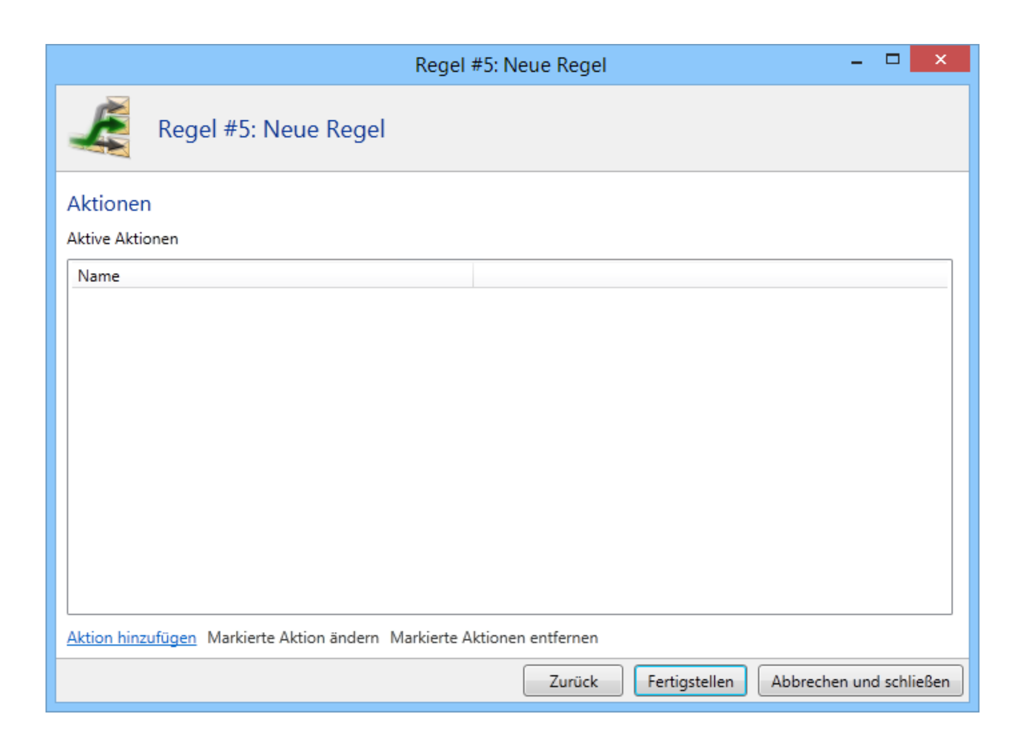


Bild 86: Die Aktionen einer E-Mail

Über den Link **Aktion hinzufügen** können Sie weitere Aktionen zur Regel hinzufügen. Je nach gewählter Aktion müssen sie diese noch konfigurieren, bevor sie zur Liste der Aktionen hinzugefügt wird. (Bild 87). Einige Aktionen sind nicht für die in der Regel gewählte Richtung funktionsfähig. Dort wird in der Spalte **Status** der Text **Kann nicht auf eingehenden (bzw. ausgehenden) Regeln angewandt werden**. Solche Aktionen können nicht hinzugefügt werden und eine Regel mit ungültigen Aktionen wird auch nicht abgespeichert.



Das Hinzufügen einer Aktion an eine Regel aufgrund der Richtung wird nur verhindert, falls sie für diese Richtung keine Funktion zeigt. Diese Beschränkung stellt nicht immer den empfohlenen Einsatz dar. Das heißt, dass Aktionen die für eine bestimmte Richtung gedacht sind, aber auch in der Gegenrichtung funktionieren, somit für beide Richtungen konfigurierbar sind. Die empfohlene Richtung steht dagegen teilweise im Namen der Aktion.

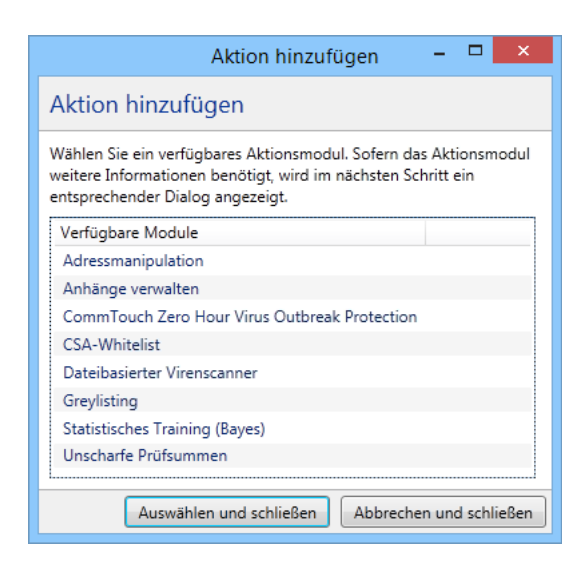


Bild 87: Aktionen aus dieser Liste können einer Regel hinzugefügt werden

Reihenfolge der Regeln ändern

Nach Beendigung des Regel-Editors erscheint die neue Regel in der Regelliste. Die Position in der Liste entspricht dem Index, den Sie im Reiter **Allgemein** des Regel-Editors festgelegt haben.

Um diese Position einer Regel zu ändern, öffnen Sie die Konfiguration der Regel und stellen Sie die neue Position über die Einstellung **Regel-Index** ein.

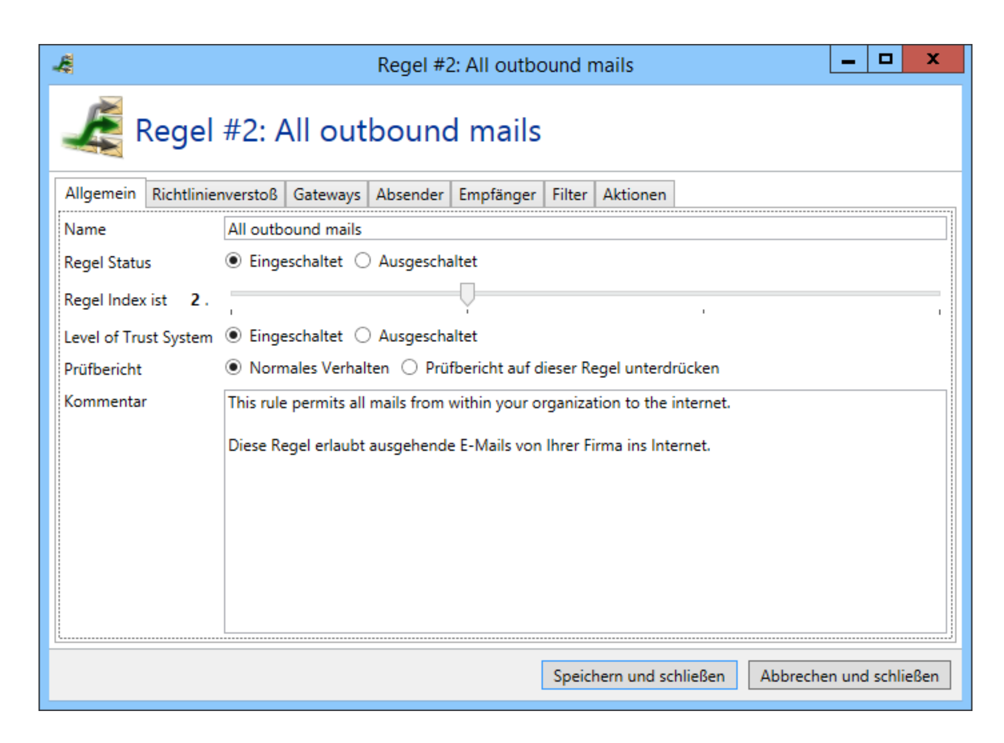


Bild 88: Über den Schieberegler für den "Regel Index" können Sie die Position der Regel verändern

Alternativ können Sie in der Linkleiste unter den Regeln auf **Regel Reihenfolge ändern** klicken. Es öffnet sich der Dialog zum Ändern der Regelreihenfolge (Bild 89).

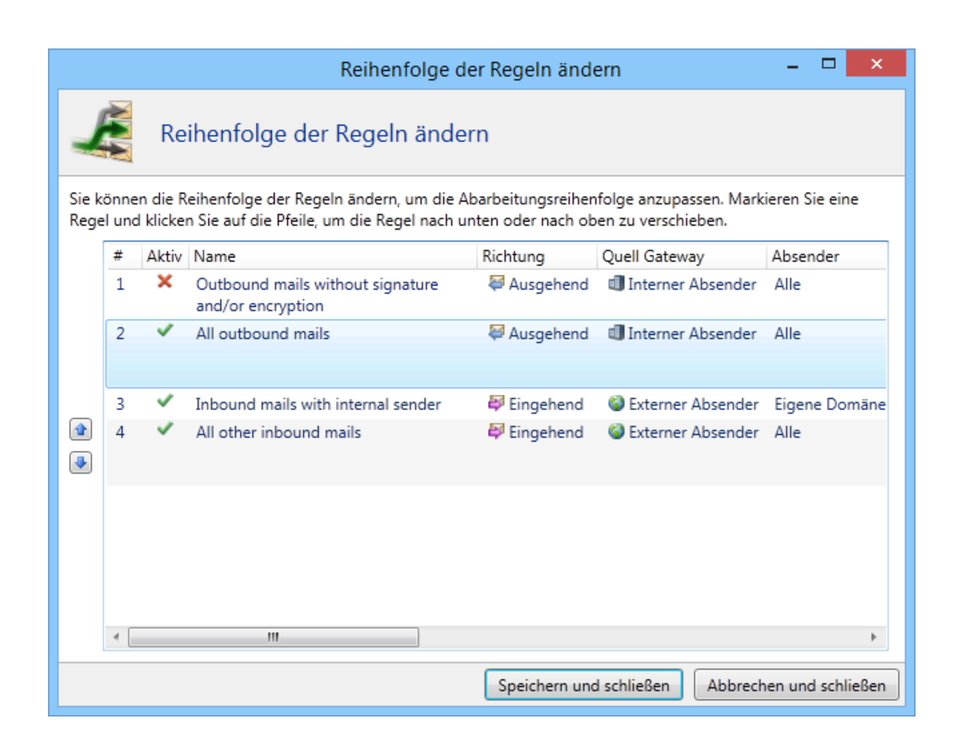


Bild 89: Hier kann die Reihenfolge aller Regeln zugleich verändert werden

Filter im Net at Work Mail Gateway

Filter bewerten E-Mails und können dadurch den Spam Confidence Level (SCL) der E-Mails beeinflussen. Dadurch kann die Entscheidung getroffen werden, ob die E-Mail abgewiesen wird, falls das Überprüfungsergebnis einen bestimmten SCL Wert übersteigt.

CYREN Anti-Spam

Anwendbar auf folgende E-Mails: **Eingehend und ausgehend**.

Der "CYREN Anti-Spam"-Filter erstellt anhand festgelegter Kriterien einen Fingerabdruck der zu prüfenden E-Mail und vergleicht ihn mit bereits vorhandenen Fingerabdrücken im lokal vorgehaltenen Cache. Befindet sich der Fingerabdruck nicht im Cache, wird eine Anfrage an ein Cyren Detection Center im Internet geschickt. Sowohl die Antwort vom lokalen Cache, als auch die Antwort vom Cyren Detection Center lautet entweder „Nein, der Fingerabdruck ist nicht bekannt“ oder „Ja, der Fingerabdruck ist bekannt“. Falls er bekannt sein sollte bedeutet das, dass Cyren die E-Mail als Spam-E-Mail einstuft. Der "Cyren Antispam"-Filter wird daraufhin 4 SCL Punkte vergeben. Der Filter selber verfügt über keine weiteren Einstellungsmöglichkeiten. Lediglich über die Gewichtung kann der Administrator weiteren Einfluss auf das Filterergebnis ausüben.

Erlaubte Unicode Sprachbereiche

Anwendbar auf folgende E-Mails: **Eingehend und ausgehend**.

E-Mails, die Spam enthalten, kommen teilweise aus Sprachräumen mit denen man generell keine Kommunikation unterhält. So kann zum Beispiel Spam eintreffen, der chinesische Schriftzeichen enthält. Dieser Filter kann E-Mails abblocken, in dem er alle enthaltenen Zeichensätze analysiert und die E-Mail nur passieren lässt, wenn alle enthalten Zeichensätze von Ihnen explizit erlaubt wurden.

Fügen Sie den Filter **Erlaubte Unicode Sprachbereiche** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration (Bild 90).

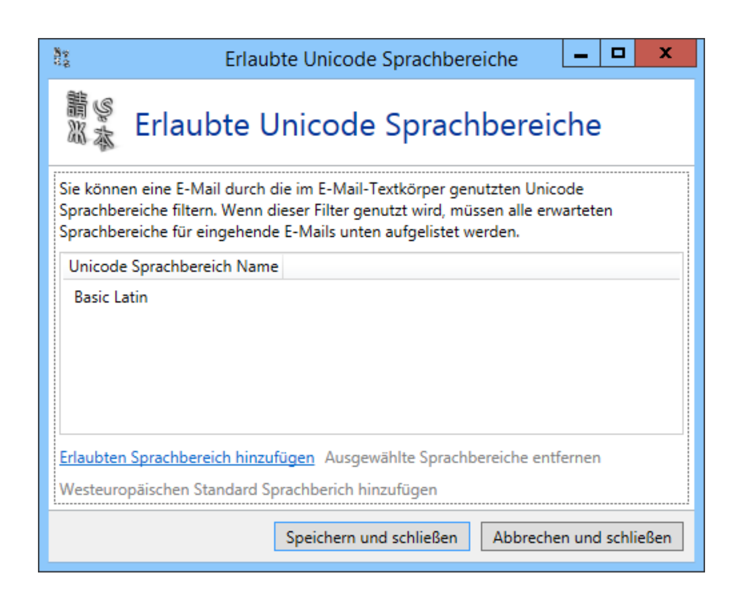


Bild 90: Die Liste der erlaubten Unicode Sprachbereiche

Fügen Sie nun alle Sprachbereiche, die in eintreffenden E-Mails verwendet werden können, zu den erlaubten Sprachbereichen hinzu. Wählen Sie dazu **Erlaubten Sprachbereich hinzufügen**. Es erscheint der Dialog mit allen noch nicht erlaubten Sprachbereichen (Bild 91).

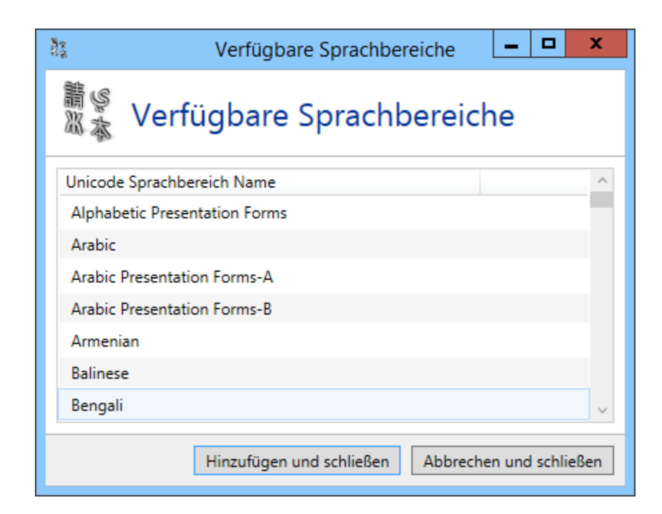


Bild 91: Die Liste der verfügbaren Unicode Sprachbereiche

Falls Sie nur mit Westeuropa oder Amerika kommunizieren, reicht üblicherweise der Sprachbereich für Westeuropäische Sprachen. Diesen können Sie, falls er sich noch nicht in der Liste der erlaubten Sprachen befindet, über **Westeuropäischen Standard Sprachbereich hinzufügen** in die Liste einfügen. (Dieser Befehl entspricht dem manuellen hinzufügen von "Basic Latin" aus der Liste der verfügbaren Sprachbereiche.)

Realtime Blocklists

Anwendbar auf folgende E-Mails: **Eingehend**.

Der Filter „Realtime Blocklists“ prüft, ob ein Adresseintrag in Realtime-Blocklists vorliegt. Sie können mehrere verschiedene Blocklists auswählen. Da auch die besten Listen False Positives aufweisen können, sollten Sie stets mehrere Listen heranziehen. Da jeder Treffer als Maluspunkt gewertet wird, wird das Risiko für eine Mail minimiert, anhand einer einzelnen Sperrliste gleich durch ein "False positive" blockiert zu werden.

Fügen Sie den Filter **Realtime Blocklists** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration (Bild 92).

Beim Filter **Realtime Blocklists** können Sie einstellen, welche Blocklists herangezogen werden sollen und welches Timeout dabei gilt. Genau wie beim Filter **Wortübereinstimmungen**, werden die einzelnen Listen global im Menü **Allgemein Filtereinstellungen** vorkonfiguriert und müssen im Filter lediglich ausgewählt werden.

Über den Link **Mit Standardlisten ersetzen** können Sie die aktuell ausgewählten Listen durch die von Net at Work empfohlenen Listen ersetzen.

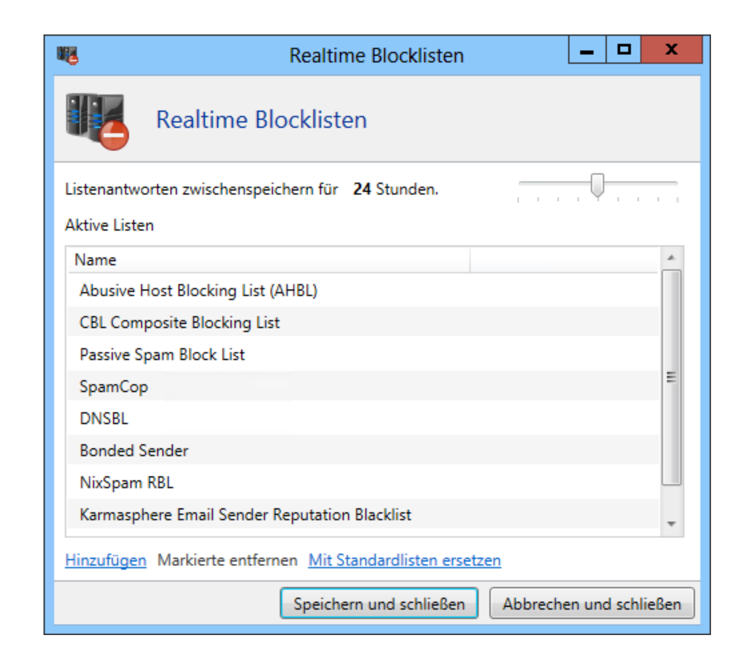


Bild 92: Fügen Sie alle Blocklists hinzu, die URIs in E-Mails überprüfen sollen

Zunächst legen Sie mit dem Schieberegler **Antworten von Listen werden für ... zwischengespeichert** fest, wie lange NoSpamProxy die Antworten der einzelnen Blocklists zwischenspeichern soll. Damit reduzieren Sie den Datenverkehr zwischen NoSpamProxy und den Blocklists erheblich und sorgen nebenbei für wesentlich schnellere Antwortzeiten bei der Abarbeitung der Blocklists.

Klicken Sie auf **Blocklist hinzufügen**, um die Blocklists auszuwählen, die NoSpamProxy bei der Filterung abfragen soll. Es öffnet sich der Dialog **Blocklist hinzufügen** (Bild 93). Wählen Sie hier die

gewünschte(n) Blocklist(s) aus und klicken anschließend auf **Hinzufügen**. In der Übersicht der Realtime Blocklists tauchen die zuvor ausgewählten Listen auf.

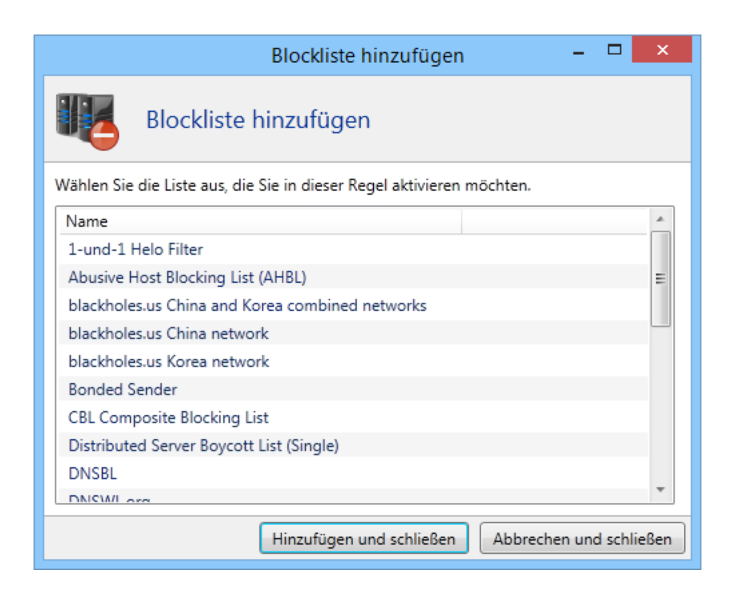


Bild 93: Sie können aus allen definierten Blocklists auswählen

Um eine oder mehrere Listen zu entfernen, markieren Sie die zu löschenden Einträge und klicken auf **Markierte Einträge** entfernen.

Beachten Sie, dass die entfernten Listen nur aus der gerade editierten Regel entfernt werden. In den globalen Regeleinstellungen tauchen die Listen nach wie vor auf.

Damit die DNS-Abfragen korrekt funktionieren, müssen Sie die DNS-Einstellungen des Betriebssystems geeignet konfigurieren. Der Server muss externe Domänen auflösen können. Es kann sinnvoll sein, einen eigenen DNS-Server als Forwarder zu installieren.

Spam URI Realtime Blocklists

Anwendbar auf folgende E-Mails: **Eingehend und ausgehend**.

Spam URI Realtime Blocklists verwalten Listen mit verdächtigen Spam-URLs. Über das Internet ist es möglich zu überprüfen, ob gegebenenfalls eine URL in dieser Liste vorhanden ist oder nicht.

Der „Spam URI Realtime Blocklists Filter“ isoliert aus den Links in einer Mail die Domäne und prüft, ob ein entsprechender Eintrag in diesen Listen vorliegt. Des Weiteren sucht er auch nach Adressen die mit „www.“ anfangen und nicht als Link in der Mail auftauchen.

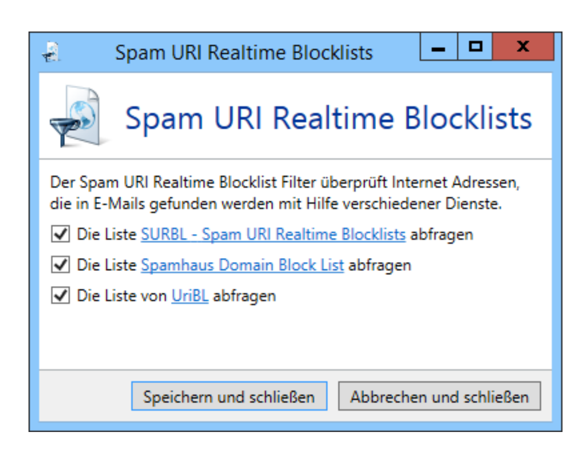


Bild 94: Konfigurieren Sie den Spam URI Realtime Blocklists Filter

Sie können mehrere verschiedene Blocklists auswählen (Bild 94).

Wie beim Realtime Blocklist Filter müssen DNS-Abfragen korrekt funktionieren. Der Server muss den angegebenen Lookup Server auflösen können. Es kann sinnvoll sein, einen eigenen DNS-Server als Forwarder zu installieren.

SpamAssassin Konnektor

Anwendbar auf folgende E-Mails: **Eingehend und ausgehend**.

SpamAssassin ist ein kostenfreier Spamfilter, welcher primär in Programmen von Universitäten und anderen kostenfreien Programmen verwendet wird. Er beinhaltet verschiedene vordefinierte Tests, um Nachrichten zu klassifizieren. Viele dieser Tests, wie z. B. RBL, führt NoSpamProxy selbst schon sehr viel früher und effektiver aus. Dennoch kann es interessant sein, die sonstigen Regeln dieses Filters zu integrieren.

SpamAssassin ist eine in Perl entwickelte Software, die eine komplette Nachricht klassifiziert, die Bewertung in den Header der Nachricht einpflegt und dem aufrufenden Prozess die veränderte Nachricht zurückgibt. Er ist daher keine eigenständige Lösung, sondern benötigt immer einen Server, in den der SpamAssassin Daemon (SpamD) integriert wird. Dieser Server bietet eine IP-Schnittstelle an, auf der der Daemon Verbindungen annimmt. Der Filter von NoSpamProxy agiert als SpamAssassin Client (SpamC) und funktioniert nur in Verbindung mit einem SpamAssassin Daemon (SpamD).

Sie können den SpamAssassin Daemon auf einem System Ihrer Wahl installieren. Dies kann ein UNIX oder Windows-System sein. Auch der Betrieb direkt auf dem gleichen Server wie NoSpamProxy ist möglich.

Fügen Sie den Filter **SpamAssassin Konnektor** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration (Bild 95).

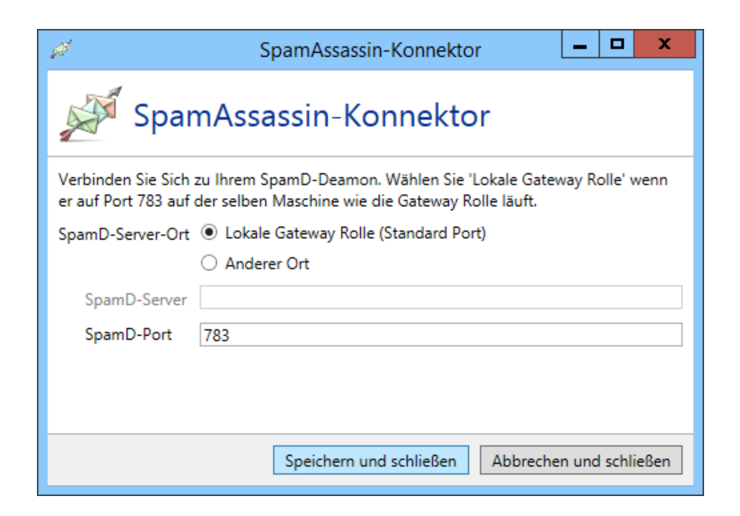


Bild 95: Definieren Sie die Verbindung zum SpamD Server

Beim SpamAssassin Konnektor können Sie die IP-Adresse bzw. den full qualified domain name (FQDN) des SpamD-Servers einstellen. Der Standard-Port des SpamD-Servers ist „783“ und kann verändert werden, wenn ihr SpamD auf einem anderen Port Verbindungen annimmt.

Mit der Einstellung **SpamD Servername** können Sie zunächst festlegen, ob sich der SpamD Server auf derselben Maschine befindet oder auf einer entfernten Maschine.

Unter **SpamD Server** können Sie die IP-Adresse bzw. den DNS-Namen des SpamD-Servers angeben. Unter **SpamD Port** können Sie die Portnummer des SpamD-Servers angeben. Standardmäßig nimmt der SpamD-Server auf der Portnummer „783“ die Verbindungen an.



Achten Sie darauf, dass NoSpamProxy das angefragte System auch erreichen kann. Oftmals sind Portfilter, IP-Routing und Firewalls zu konfigurieren, damit NoSpamProxy den SpamD-Server auch erreichen kann.

Verhindere eigene Domänen im 'From' E-Mail-Header

Anwendbar auf folgende E-Mails: **Eingehend**.

Einige Spam-E-Mails fügen einen Absender aus den lokalen Domänen in den 'From'-E-Mail-Header ein aber nicht in den Absender des E-Mail-Envelopes. Die Daten aus dem 'From'-Feld dienen zur Anzeige des Absenders in Ihrem E-Mail-Programm. Die manipulierten Absenderdaten sollen Vertrauen aufbauen und den Benutzer motivieren, die E-Mail zu öffnen. Solche E-Mails werden zunächst nicht von der Standardregel "Inbound mails with internal sender" erfasst, da diese Regel nur die Adressdaten aus dem E-Mail-Envelopes analysiert. Sollen solche E-Mails dennoch blockiert werden, können Sie diesen Filter benutzen.



Einige Mailing-Listen setzen den Empfänger der E-Mail in den 'From'-Header ein. Derartige E-Mails werden von diesem Filter ebenfalls als Spam bewertet.

Wortübereinstimmungen

Anwendbar auf folgende E-Mails: **Eingehend und ausgehend**.

Mit diesem Filter können Sie vorher definierte Wörter und Ausdrücke sowohl in der Betreffzeile als auch dem E-Mail-Body erkennen und sie mit positiven oder negativen SCL-Punkten bewerten. Jedes Auftauchen, oder je nach Einstellung auch Fehlen, eines solchen Ausdrucks in einer E-Mail wird mit den im Filter eingestellten Punkten bewertet.



Die in diesem Filter zur Verfügung stehenden Wortgruppen werden zuvor unter dem Knoten Allgemeine Regeleinstellungen definiert.

Fügen Sie den Filter **Wortübereinstimmungen** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration (Bild 96).

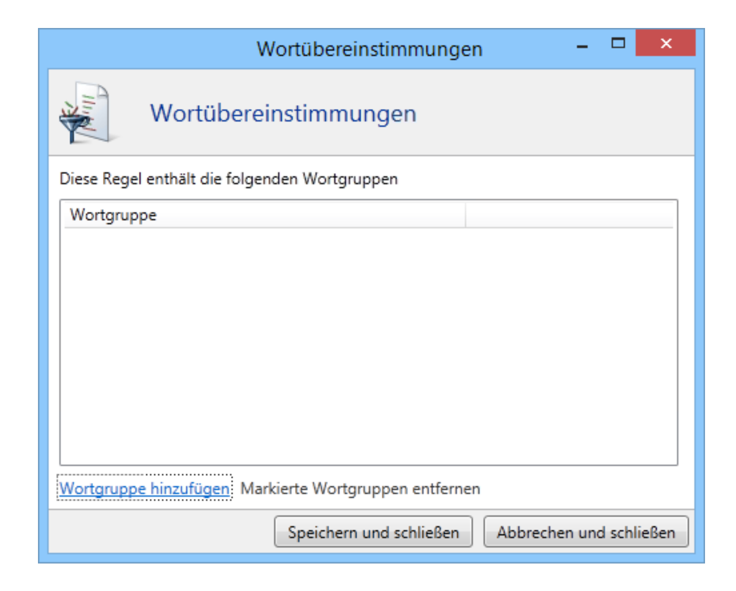


Bild 96: Fügen Sie Ihre definierten Wortgruppen in den Filter der Wortübereinstimmungen ein

Nun haben Sie die Möglichkeit über den Link **Wortgruppe hinzufügen**, zuvor erstellte Wortgruppen aufzunehmen. Standardmäßig sind bereits einige Wortgruppen vorkonfiguriert. Wählen Sie die gewünschte(n) Wortgruppe(n) aus und klicken Sie auf **Hinzufügen**. In der Übersicht des Dialogs für die Wortübereinstimmungen sehen Sie nun die ausgewählten Wortgruppen.

Aktionen im Net at Work Mail Gateway

Aktionen können E-Mails verändern

Nachdem die Filter von NoSpamProxy verarbeitet wurden und eine Spam-Bewertung berechnet ist, startet das Net at Work Mail Gateway die eingestellten Aktionen. Eine Aktion erhält Informationen über das Filter-Ergebnis und kann daraufhin weitergehende Aufgaben ausführen. Im Gegensatz zu den Filtern können Aktionen die E-Mails verändern; zum Beispiel Anhänge aussortieren. Zudem können Aktionen Filter-Ergebnisse überstimmen. Beispiele hierfür sind Virenscanner und eine Greylisting Aktion.

Um eine Aktion zu aktivieren, müssen Sie in der Regel, die die Aktion enthalten soll, die Karteikarte **Aktionen** wählen. Dann klicken Sie auf **Aktion hinzufügen**. Es erscheint der Dialog **Aktion hinzufügen** in dem Sie die hinzuzufügende Aktion auswählen und dann auf **Auswählen und schließen** klicken. Nun wird die Aktion hinzugefügt, oder falls sie konfiguriert werden muss, die Konfiguration der Aktion geöffnet und die Aktion danach zu Ihrer Regel hinzugefügt.

Adressmanipulation

Anwendbar auf folgende E-Mails: **Eingehend und ausgehend**.

Diese Aktion eröffnet Ihnen die Möglichkeit, die Zieladresse beim Empfang einer E-Mail zu verändern. So können Sie z. B. nach einem Namenswechsel der Firma, alle E-Mails, die an die alte Adresse adressiert sind, an die neue Adresse umschreiben lassen.

Ein zweiter Anwendungsfall ist die Definition einer „Geheimadresse“. So können Sie zum Beispiel festlegen, dass alle eingehenden E-Mails mit einem Zusatz *geheim* im Adressfeld, als erwünscht bewertet und im „Pass“-Modus durchgelassen werden. Eine Regel könnte wie folgt aussehen:

Pos.	Von	An	Entscheidung	Aktion
1	*@*	*geheim@example.com	Pass	Adressmanipulation

Die Adressmanipulation entfernt das „Code“-Wort und leitet diese E-Mail an Ihre korrekte E-Mail-Adresse weiter. Das „Code“-Wort in der Adresse können Sie natürlich selbst festlegen und bei Bedarf wieder ändern.

Fügen Sie die Aktion **Adressmanipulation** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration (Bild 97).

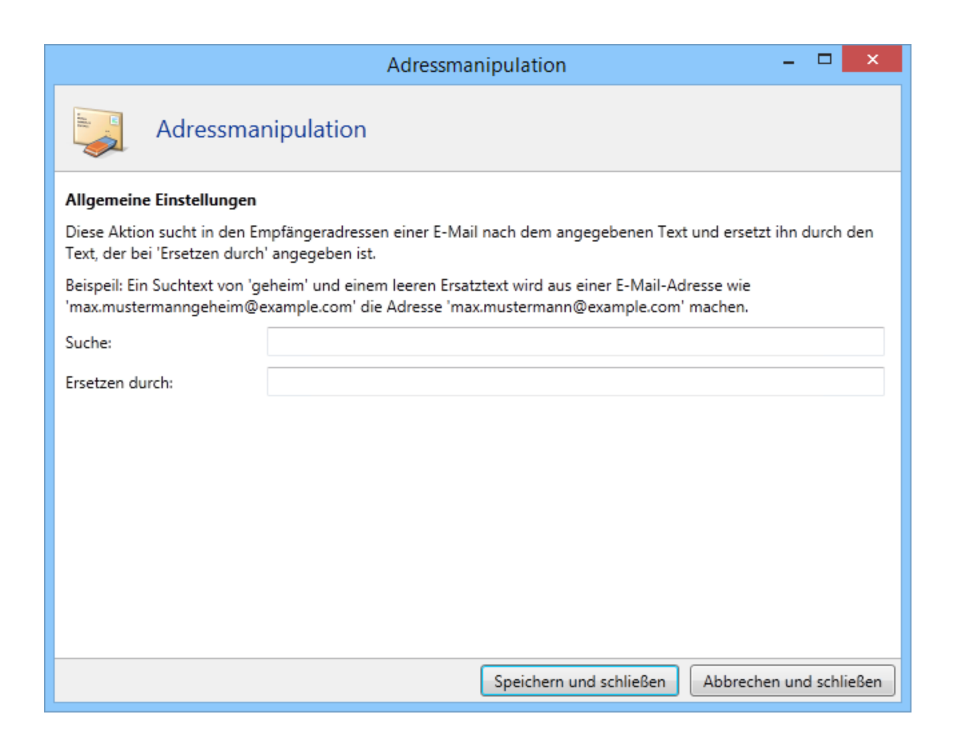


Bild 97: Konfigurieren Sie Ersetzungen auf den Empfänger Adressen der E-Mails

Sie können angeben, welcher Teil einer "Code"-Wort-Adresse durch einen Teil der korrekten Adresse ersetzt werden soll.

In den **Allgemeinen Einstellungen** tragen Sie unter **Suchen** den zu ersetzenden String aus der „Geheim"-Adresse ein, für die die Adressmanipulation aktiv werden soll.

Unter **Ersetzen durch** geben Sie ein, mit welchem Text der Text aus dem Feld **Suchen** ersetzt werden soll.

So ist es beispielsweise sinnvoll, den String „topsecret" in der „Geheim"-Adresse „user1topsecret@example.com" durch einen leeren String für die korrekte Adresse „user1@example.com" zu ersetzen.

Anhänge verwalten

Anwendbar auf folgende E-Mails: **Eingehend und ausgehend**.

Die Aktion „Anhänge verwalten" prüft die Dateinamen der Anhänge und löscht relevante Anhänge oder weist die zugehörigen E-Mails ab. Alternativ können Anhänge auch auf das Web Portal verschoben werden. So können Sie beispielsweise alle E-Mails mit „*.exe"-Dateien abweisen oder nur die Anlage löschen. Alternativ können Sie auch einstellen, dass Sie generell alle E-Mails mit Anhängen abweisen möchten, außer E-Mails, mit von Ihnen festgelegten Anhängen (Whitelisting).

Prinzipiell ist es eine sehr gute Idee, ausführbare Anlagen in E-Mails von vornherein abzuweisen. Im alltäglichen Geschäftsverkehr werden zwar sehr viele Dokumente und andere Dateien ausgetauscht, jedoch in der Regel keine Programme. Sollte der Austausch von ausführbarem Code erforderlich sein, ist es heute nicht zu viel verlangt, diese Dateien in ein Archiv zu verpacken. Sehr viele Viren verbreiten

sich über Programm-Anhänge, weil Anwender unbedarft Anlagen direkt ausführen. Dies wird durch eine solche Blockade verhindert.

In der Aktion „Anhänge verwalten“ können Sie eintragen, welche Anhänge aussortiert werden sollen und wie mit der zugehörigen E-Mail verfahren werden soll.

Ein typisches Beispiel sind die „*.exe“-Dateianhänge. Sie können festlegen, ob Anhänge dieses Typs aus den E-Mails herausgenommen werden oder ob E-Mails, die einen solchen Anhang aufweisen, abgewiesen werden sollen.

Im Konfigurationsdialog sehen Sie die konfigurierten Einträge. Diese werden für jeden Anhang, analog zu den Regeln, von oben nach unten abgearbeitet, bis ein für den Anhang passender Eintrag gefunden wird. Wird kein Eintrag gefunden, bleibt der Anhang unverändert an der E-Mail. Wie bei den Regeln können Sie die Reihenfolge über die Schaltflächen mit den Pfeilen links neben der Liste beeinflussen (Bild 98).

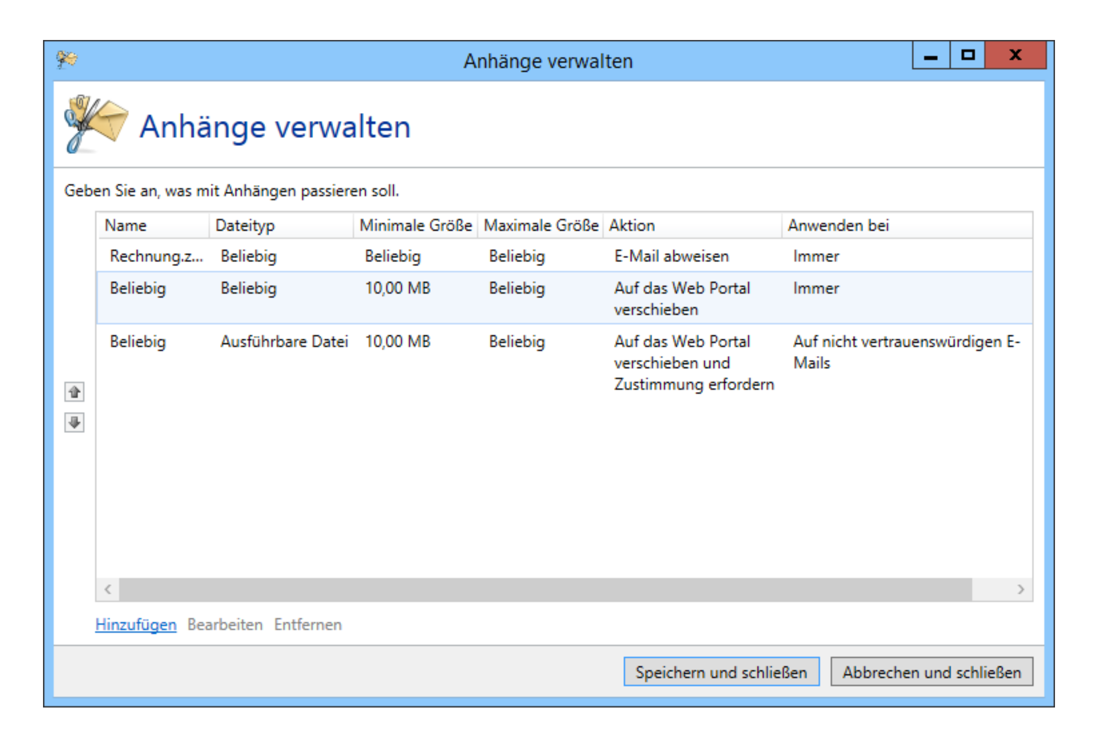


Bild 98: Konfigurieren Sie, wie Anhänge verarbeitet werden

Jeder Eintrag besteht aus drei Teilen (Bild 99):

- **Bedingung**
  Wählen Sie hier aus, für welche Anhänge der Eintrag gelten soll. Sie können einen Anhang über den Namen, Inhaltstyp und Größe beschreiben. Wählen Sie keine Bedingung aus, dann gilt der Eintrag für alle Anhänge.
- **Aktion**
  Wählen Sie hier aus, was mit dem Anhang passieren soll: E-Mail abweisen, Anhang von der E-Mail entfernen, Anhang auf das Web Portal hochladen und duch einen Link ersetzen oder an der

E-Mail lassen. Falls Sie die Aktion auf einer Regel für eingehende Nachrichten einsetzen, dann können Sie auch noch angeben, dass der Anhang zusätzlich zum Hochladen auf das Web Portal auch noch gesperrt wird. In diesem Fall kann der Empfänger den Anhang nur herunterladen, wenn er von einem Administrator freigegeben wurde.

- **Level of Trust**
  Unter diesem Punkt können Sie wählen, ob der Eintrag auch auf E-Mails angewandt wird, die vom Level-of-Trust-System als vertrauenswürdig eingestuft wurden, oder ob der Eintrag für solche E-Mails ignoriert wird.



Hat eine E-Mail mehrere Anhänge, dann kann folgendes Szeanrio vorkommen: Bei Anhang 1 soll der Anhang entfernt werden, bei Anhang 2 jedoch die E-Mail abgewiesen werden. Letzeres wiegt schwerer, daher wird die E-Mail in diesem Fall abgewiesen.

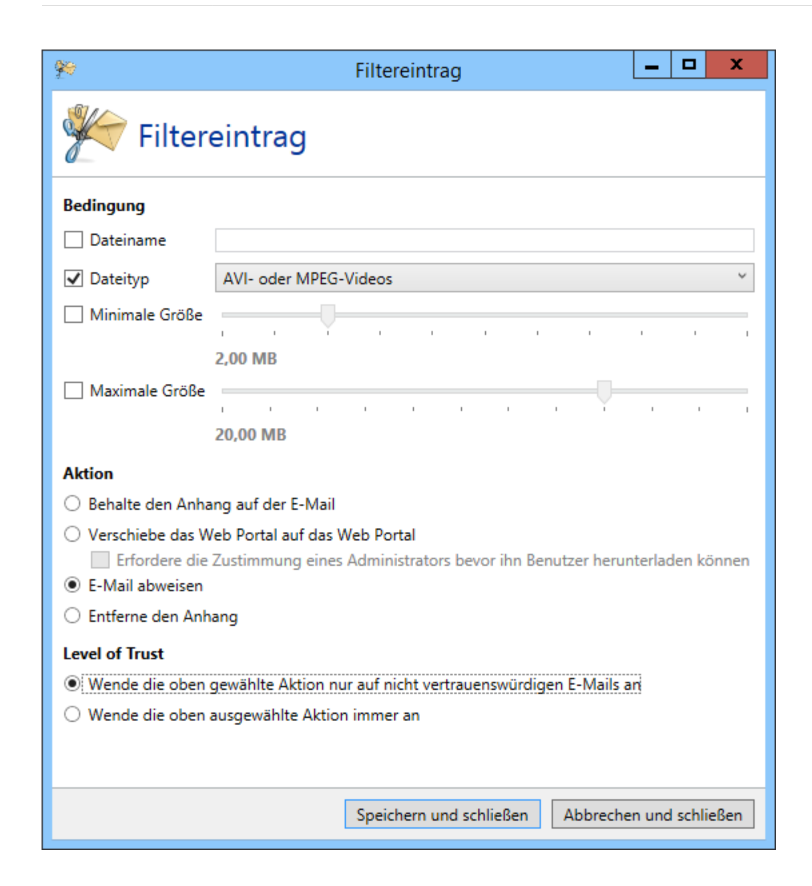


Bild 99: Filtereintrag für Anhänge

CYREN Premium Antivirus

Anwendbar auf folgende E-Mails: **Eingehend und ausgehend**.

Ungeachtet der Filterergebnisse erstellt die "CYREN Antivirus"-Aktion anhand festgelegter Kriterien einen Fingerabdruck der zu prüfenden E-Mail und vergleicht ihn mit bereits vorhandenen Fingerabdrücken im lokal vorgehaltenen Cache. Befindet sich der Fingerabdruck nicht im Cache, wird

eine Anfrage an ein CYREN Detection Center im Internet geschickt. Sowohl die Antwort vom lokalen Cache, als auch die Antwort vom CYREN Detection Center lautet entweder „Nein, der Fingerabdruck ist nicht bekannt“ oder „Ja, der Fingerabdruck ist bekannt“. Falls er bekannt sein sollte bedeutet das, dass CYREN die E-Mail als Virus-Mail einstuft. Zusätzlich wird die vollständige E-Mail mit lokal vorgehaltenen Pattern-Dateien auf alle bekannten Viren hin überprüft.

CSA-Whitelist

Anwendbar auf folgende E-Mails: **Eingehend**.

Viele Newsletter sind erwünscht, da ihre Inhalte mit Zustimmung des Empfängers ausgeliefert werden. Das Problem an solchen Newslettern ist, dass der Empfang nicht sichergestellt werden kann, da bisher kein Level-of-Trust-Eintrag automatisch erstellt wurde und es ein zu großer Aufwand ist, alle vertrauenswürdigen Newsletter-Versender manuell als vertrauten Partner einzutragen.

Diese Lücke schließt die CSA-Whitelist. Sie stellt eine Positiv-Liste dar, bei der ein Kontrollgremium die Rechtmäßigkeit der versendeten Newsletter überwacht. Dadurch können Newsletter von Versendern, die sich auf der CSA-Whitelist befinden, gefahrlos zugestellt werden.

Wenn sich der Absender einer empfangenen E-Mail in der CSA-Whitelist befindet, markiert die CSA-Whitelist Aktion die E-Mail als vertrauenswürdig. Dadurch werden alle Filter der angewandten Regeln übersprungen.

Fügen Sie die Aktion **CSA-Whitelist** an Ihre Regel an. Sie erscheint danach in der Aktionsübersicht der Regel.

Die Konfiguration der Aktion wird unter den Allgemeinen Regeleinstellungen vorgenommen.

Dateibasierter Virenscanner

Anwendbar auf folgende E-Mails: **Eingehend und ausgehend**.

Viren sind, neben Spam, eine große Bedrohung und sollten ebenfalls so früh wie möglich aussortiert werden. Auch bei der Suche nach Viren können übereifrige Filter eine erwünschte E-Mail irrtümlich entfernen. Die meisten Produkte löschen solche E-Mails, ohne den Empfänger oder Absender zu informieren. Die Problematik ist hier vergleichbar mit einem Quarantäneverzeichnis einer herkömmlichen Lösung. NoSpamProxy arbeitet anders.

Die Aktion „Dateibasierter Virenscanner“ speichert Anhänge von durchkommenden E-Mails in ein bestimmtes Verzeichnis. Wenn Sie einen beliebigen OnAccess-Virusscanner installiert haben, wird dieser Scanner einen lesenden Zugriff auf eventuell verseuchte Anhänge verweigern. NoSpamProxy prüft sofort nach Ablage der Anhänge in das Verzeichnis, ob ein Zugriff möglich ist oder nicht. Anhänge, auf die zugegriffen werden kann, werden als virenfrei angesehen. NoSpamProxy kann mit jedem beliebigen Virenscanner zusammen arbeiten, der in Echtzeit Dateizugriffe überwacht. Diese Scanmethode ist auf sehr vielen Dateiservern bereits installiert, sehr performant und zuverlässig.

Sie können selbst einstellen, ob verseuchte Anhänge nur gelöscht werden oder ob die zugehörige E-Mail automatisch geblockt werden soll.



Falls eine E-Mail abgewiesen wird, wird der Absender darüber durch den einliefernden Server informiert. Über einen gelöschten Anhang wird weder der Absender noch der Empfänger informiert.

Fügen Sie die Aktion **Dateibasierter Virenscanner** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration (Bild 100).

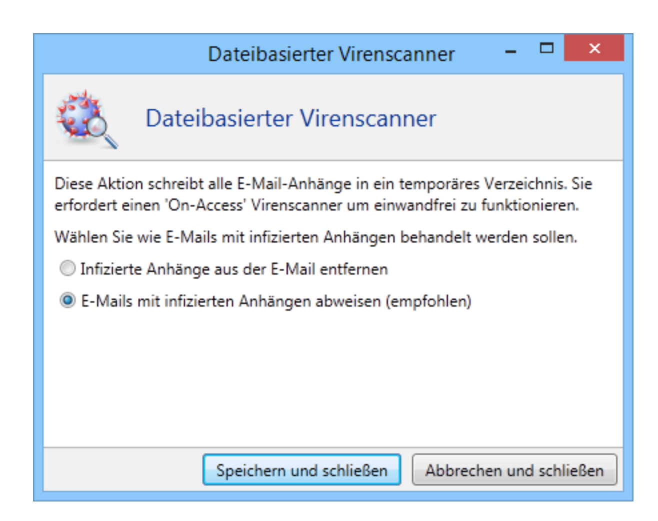


Bild 100: Konfigurieren Sie die Aktion für den dateibasierten Virenscanner

Wenn Sie diese Art von E-Mails ablehnen, dann wird, wie bei einer erkannten Spam-E-Mail, der einliefernde E-Mail-Server eine Unzustellbarkeitsnachricht abschicken. Das Risiko bei einer Falscherkennung entfällt.

In der Dateibasierten Virenscanner Aktion können Sie festlegen, wie mit verseuchten Anhängen und der zugehörigen E-Mail verfahren wird.

Wählen Sie aus, ob infizierte Anhänge aus der E-Mail entfernt werden sollen oder ob E-Mails mit infizierten Anhängen abgewiesen werden sollen. Die Aktion wird nun in der Übersicht der Aktionen in der Regel angezeigt.



Wie bei allen Virenscannern, werden auch hier kennwortgeschützte Zip-Dateien nicht überprüft und ohne weitere Prüfung weitergegeben.

Greylisting

Anwendbar auf folgende E-Mails: **Eingehend**.

Das Greylisting ist eine Vorsichtsmaßnahme gegen „verdächtige“ E-Mails. Bleibt eine E-Mail knapp unter dem von Ihnen definierten Spam-Schwellenwert, würde diese E-Mail ohne Greylisting als ausreichend

gut bewertet werden. Die Greylisting-Aktion lässt nun diese E-Mail nicht gleich durch, sondern lehnt sie temporär ab. Der einliefernde E-Mail-Server bekommt eine Fehlermeldung, die ihn dazu bewegt, die E-Mail nach einiger Zeit erneut zu senden. Im zweiten Versuch wird die E-Mail dann zugestellt. Dabei kann eingestellt werden, ab wann der einliefernde Server einen zweiten Versuch starten darf.

Hinter dieser Aktion steht folgendes Prinzip: Ein Spammer scheut in der Regel die Mühe, eine zweite E-Mail zu senden. Ein normaler Absender hingegen wird nach einiger Zeit erneut die Zustellung versuchen. Bei dem zweiten Versuch wird nun diese Verbindung besser bewertet, so dass die E-Mail passieren kann.

Den Schwellenwert, ab wie vielen Malus-Punkten eine eigentlich passierende E-Mail als „verdächtig" eingestuft wird, können Sie individuell einstellen.

Fügen Sie die Aktion **Greylisting** an Ihre Regel an. Es öffnet sich der Dialog für die Konfiguration (Bild 101).

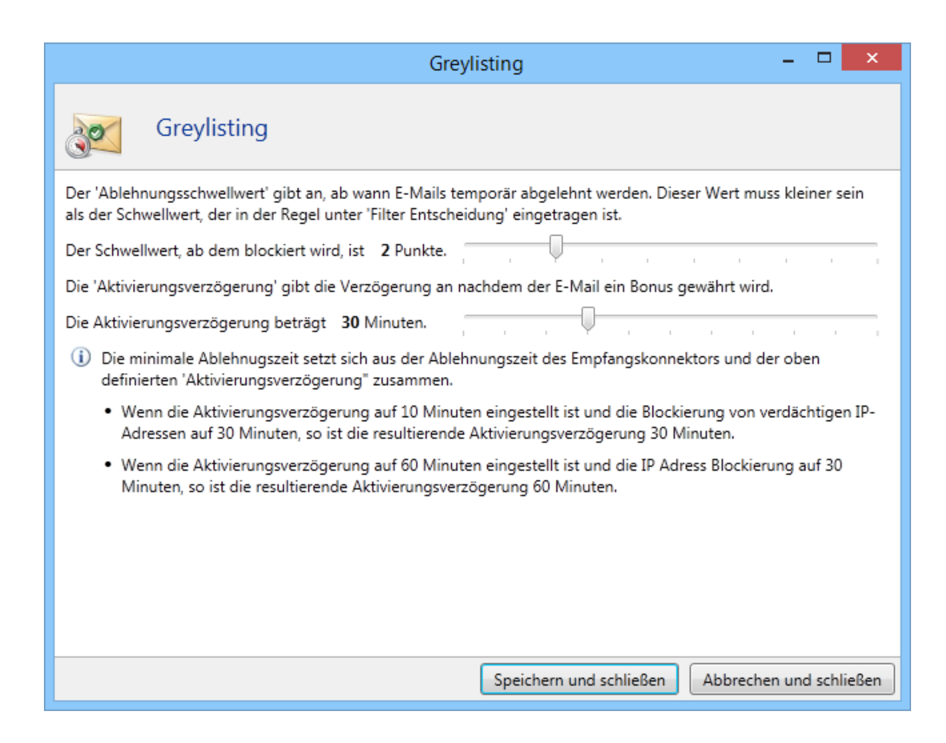


Bild 101: Konfigurieren Sie die Optionen des Greylisting

Sie können angeben, ab welchem Schwellenwert das Greylisting aktiv wird und die Verzögerungszeit einstellen, nach der der Level-of-Trust-Eintrag erfolgen soll.

Mit dem Schieberegler **Der Schwellwert, ab dem blockiert wird** können Sie angeben, ab welchem Schwellenwert (SCL) E-Mails für das Greylisting zwischenzeitlich geblockt werden sollen. Dieser Greylisting-Schwellenwert muss niedriger sein als der Spam-Schwellenwert, andernfalls würde das Greylisting nicht greifen.

Des Weiteren können Sie die **Aktivierungsverzögerung** ändern. Damit bestimmen Sie die Verzögerungszeit, nach der die E-Mail besser bewertet wird.



Verwenden Sie die Greylisting-Aktion nur in Verbindung mit der Level-of-Trust-Aktion.

Verberge interne Topologie

Anwendbar auf folgende E-Mails: **Ausgehend**.

Die Aktion **Verberge interne Topologie** entfernt die "Received"-E-Mail-Header einer ausgehenden E-Mail. Durch diese Received-Einträge kann ansonsten ein Rückschluss auf die interne Topologie erfolgen.

Berechnung des Spam Confidence Level

Das Net at Work Mail Gateway mit NoSpamProxy weist alle E-Mails ab, deren Spam Confidence Level (SCL) über einem bestimmten Schwellwert liegt. Diesen Schwellwert legen Sie als Administrator in den einzelnen Regeln fest. Der folgende Absatz erläutert die Vorgehensweise von NoSpamProxy bei der Berechnung des SCL. Zunächst wird an einem sehr einfachen Beispiel erläutert, wie die Filter ohne das Level-of-Trust-System arbeiten. Die folgende Filterkonfiguration ist dabei gegeben (Bild 102).

E-Mail überprüfen
Abweisen wenn SCL ist größer 4

Realtime Blocklists (2)
Spam URI Realtime Blocklists (2)
Wortübereinstimmungen (1)

Bild 102: Die Beispielkonfiguration für die Berechnung des SCL Wertes

In diesem Beispiel sollen E-Mails überprüft und abgewiesen werden, sobald der SCL größer oder gleich 4 ist. Es sind drei Filter aktiviert: Realtime Blocklists, Spam URI Realtime Blocklists und die Wortübereinstimmungen. Der Filter Wortübereinstimmungen ist so konfiguriert, dass er nach den Wörtern Sex, Viagra, Cialis etc. suchen und pro Treffer zwei Strafpunkte vergeben soll. Die beiden Blocklistfilter sollen pro Treffer zwei Punkte vergeben. Das Level-of-Trust-System ist ausgeschaltet.

Nun wird eine Mail verarbeitet, die acht verbotene Wörter und einen verbotenen Link enthält. Der Link ist auf einer Blacklist enthalten. Des Weiteren ist die einliefernde IP-Adresse auf zwei Blacklists vertreten. Hier zunächst das vorläufige Ergebnis der Filter:

Filter	SCL Bewertung des Filters
Realtime Blocklists	4 (Zwei Treffer X zwei Strafpunkte pro Treffer)
Spam URI Realtime Blocklists	2 (Ein Treffer X zwei Strafpunkte pro Treffer)

Wortübereinstimmungen	16 (Acht Treffer X zwei Strafpunkte pro Treffer)

Grundsätzlich ist es bei allen Filtern, auch dem Level-of-Trust-System so, dass der ermittelte Wert immer auf 10 zurückgekürzt wird, wenn er größer als „10“ ist. Bei negativen Werten die kleiner als „-10“ sind, wird der Wert auf -10 angepasst. In unserem Beispiel wäre dann der Nettowert der Filter wie folgt:

Filter	**SCL Bewertung des Filters**
Realtime Blocklists	4
Spam URI Realtime Blocklists	2
Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)

Abschließend wird die Gewichtung der einzelnen Filter berücksichtigt. Die Filter Realtime Blocklists und Spam URI Realtime Blocklists haben die Gewichtung „2“, die Wortübereinstimmungen haben die Gewichtung „1“. Der Nettowert der Filter wird nun mit der jeweiligen Gewichtung multipliziert. Folgende Werte ergeben sich nun:

Filter	**SCL Bewertung des Filters**	**Gewichtung**	**SCL**
Realtime Blocklists	4	2	8
Spam URI Realtime Blocklists	2	2	4
Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)	1	10
Gesamt			**22**

Die E-Mail erhält also einen SCL von 22 und wird damit abgewiesen.

Im zweiten Beispiel wird die Filterkonfiguration aus dem ersten Beispiel lediglich um das Level-of-Trust-System erweitert. Es handelt sich des Weiteren um die gleiche E-Mail wie im vorigen Beispiel. Wir gehen aber davon aus, dass es sich hier um eine gewollte E-Mail handelt und es von der Absender- und Empfänger-Adresse bereits ein Adresspärchen und einen Domänenbonus in der Datenbank gibt. Da der letzte Mailkontakt bereits vier Tage her ist, ist der Adresspärchen-Bonus mit 65 Bonuspunkten nicht mehr so hoch. Die Domäne hingegen steht mit statischen 100 Bonuspunkten in den Vertrauensstellungen. Bei den Bonuspunkten des Level-of-Trust-Systems in der Datenbank handelt es sich nicht direkt um den SCL Wert, sondern um die sogenannten Trustpunkte. Diese werden nur Filter intern verwendet.

Das Level-of-Trust-System bewertet nun wie folgt:

Zunächst werden die Werte aus dem Adresspärchenbonus und dem Domänenbonus addiert und ergeben somit die Summe „165“. Zur Berechnung des SCL wird diese Summe grundsätzlich durch den

Wert „-10“ dividiert und ergibt in diesem Beispiel einen SCL von -16,5 Punkten. Wie bei allen anderen Filtern auch, wird der ermittelte Wert auf 10 oder -10 beschnitten. Die Tabelle mit den Nettowerten aller Filter sieht nun wie folgt aus:

Filter	**SCL Bewertung des Filters**
Realtime Blocklists	4
Spam URI Realtime Blocklists	2
Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)
Level-of-Trust-System	-10 (limitiert, da der erste Wert <(-10) war)

Die Gewichtung der einzelnen Filter können Sie in der jeweiligen Regel festlegen. Das Level-of-Trust-System hingegen ermittelt seine Gewichtung selbstständig. Dazu werden die Gewichtungen aller anderen Filter addiert und ergeben in diesem Beispiel den Wert „5“. Die endgültige Berechnung des SCL mit dem Einfluss des Level-of-Trust-Systems sieht dann wie folgt aus:

Filter	**SCL Bewertung des Filters**	**Gewichtung**	**SCL**
Realtime Blocklists	4	2	8
Spam URI Realtime Blocklists	2	2	4
Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)	1	10
Level-of-Trust-System	-10 (limitiert, da der erste Wert <(-10) war)	5 (=2+2+1)	-50
Gesamt			**-28**

Die E-Mail wäre in diesem Beispiel zugestellt worden, da der SCL kleiner als 4 ist.

Um das Beispiel zu verdeutlichen, wird der Filter "CYREN Antispam" mit der Gewichtung „3“ hinzu konfiguriert. Dieser Filter vergibt bei einem Treffer immer 4 Punkte und dieser Wert ist auch nicht konfigurierbar. (Bild 103)

E-Mail überprüfen
Abweisen wenn SCL ist größer 4
Realtime Blocklists (2)
Spam URI Realtime Blocklists (2)
Wortübereinstimmungen (1)
CommTouch AntiSpam Dienst (3)

Bild 103: Zur Berechnung der SCL wurde der "CYREN Antispam" Filter hinzugefügt

Der "CYREN Antispam" Filter bewertet die E-Mail ebenfalls schlecht. Das Endergebnis der SCL Berechnung sieht dann wie folgt aus:

Filter	SCL Bewertung des Filters	Gewichtung	SCL
Realtime Blocklists	4	2	8
Spam URI Realtime Blocklists	2	2	4
Wortübereinstimmungen	10 (limitiert, da der erste Wert >10 war)	1	10
CYREN Antispam	4	3	12
Level-of-Trust-System	-10 (limitiert, da der erste Wert <(-10) war)	8 (=2+2+1+3)	-80
Gesamt			**-46**

Die Gewichtung des Level-of-Trust-Systems hat sich durch den zusätzlichen Filter automatisch angepasst und kann sich dadurch noch entscheidender durchsetzt. Es wird damit gewährleistet, dass gewollte Kommunikation auch immer den Empfänger erreicht, egal welchen Inhalt die E-Mail aufweist.

Allgemeine Regeleinstellungen

Dieser Bereich beherbergt globale Einstellungen für Aktionen und Filter in den Regeln (Bild 104).

Net at Work Mail Gateway Configuration Console - [Net at Work Mail Gateway\Konfiguration\Allgemeine Regeleinstellungen]

File Action View Help

- Net at Work Mail Gateway
  - Monitoring
  - Menschen und Identitäten
  - Konfiguration
    - E-Mail-Routing
    - Regeln
    - Allgemeine Regeleinstellungen
    - Gateway Komponenten
    - Verbundene Systeme
    - Benutzer-Benachrichtigungen
    - Erweiterte Einstellungen
  - Troubleshooting

CSA-Whitelist

Die CSA-Whitelist wird alle **24** Stunden heruntergeladen.

Bearbeiten Whitelist jetzt herunterladen

Wortübereinstimmungen

Globale Wortgruppen

Name	Bereich	Suchkriterium	Format	Punkte pro Treffer
Common notation for medical products	Betreff und Inhalt	Ähnliche Wörter	Platzhalter	2
Common notation of commercial words	Betreff und Inhalt	Ähnliche Wörter	Platzhalter	2
Common notation of porn words	Betreff und Inhalt	Ähnliche Wörter	Platzhalter	2
Common spam words (german)	Betreff und Inhalt	Ähnliche Wörter	Platzhalter	2

Hinzufügen Bearbeiten Entfernen

Realtime Blocklisten

Globale Blocklisten

Name	Typ	URL
1-und-1 Helo Filter	HTTP	http://schizo-bl.kundenserver.de/?ip=[IP]
Abusive Host Blocking List (AHBL)	DNS	dnsbl.ahbl.org
Bonded Sender	DNS	query.bondedsender.org
CBL Composite Blocking List	DNS	cbl.abuseat.org
DNSBL	DNS	t1.dnsbl.net.au
DNSWL.org	DNS	list.dnswl.org
Karmasphere Email Sender Reputation Blacklist	DNS	karmasphere.email-sender.dnsbl.karmasphere.com
Karmasphere Email Sender Reputation Whitelist	DNS	karmasphere.email-sender.dnswl.karmasphere.com
NixSpam RBL	DNS	ix.dnsbl.manitu.net
No-more-funn	DNS	no-more-funn.moensted.dk
Not Just Another Bogus List (NJABL Combined List)	DNS	combined.njabl.org

Hinzufügen Bearbeiten Entfernen

Bild 104: Allgemeine Einstellungen der Regeln



Die Änderung von Einstellungen in diesem Bereich wirkt sich auch auf bestehende Regeln aus. Die Einstellungen gelten immer für alle Regeln, in denen sich die davon abhängigen Aktionen oder Filter befinden.

Realtime Blocklists

Realtime Blocklists (RBL) verwalten Listen mit verdächtigen Spam-IP-Adressen. Über das Internet ist es nun möglich zu überprüfen, ob gegebenenfalls eine IP-Adresse in der RBL-Liste vorhanden ist oder

nicht. Diese Blocklists werden im Abschnitt **Realtime Blocklists** gepflegt und können in den Regeln dann später einzeln ausgewählt werden.

Neue Blocklist hinzufügen

Unter **Allgemeine Einstellungen** (Bild 105) geben Sie im Feld **Name** zunächst den Namen der neuen RBL-Liste an. Im Feld **Beschreibung** können Sie persönliche Anmerkungen machen, damit Sie hinterher noch wissen, was es mit dieser Liste auf sich hat. Beide Einträge sind nur beschreibende Details, für die Funktion der Liste aber nicht relevant.

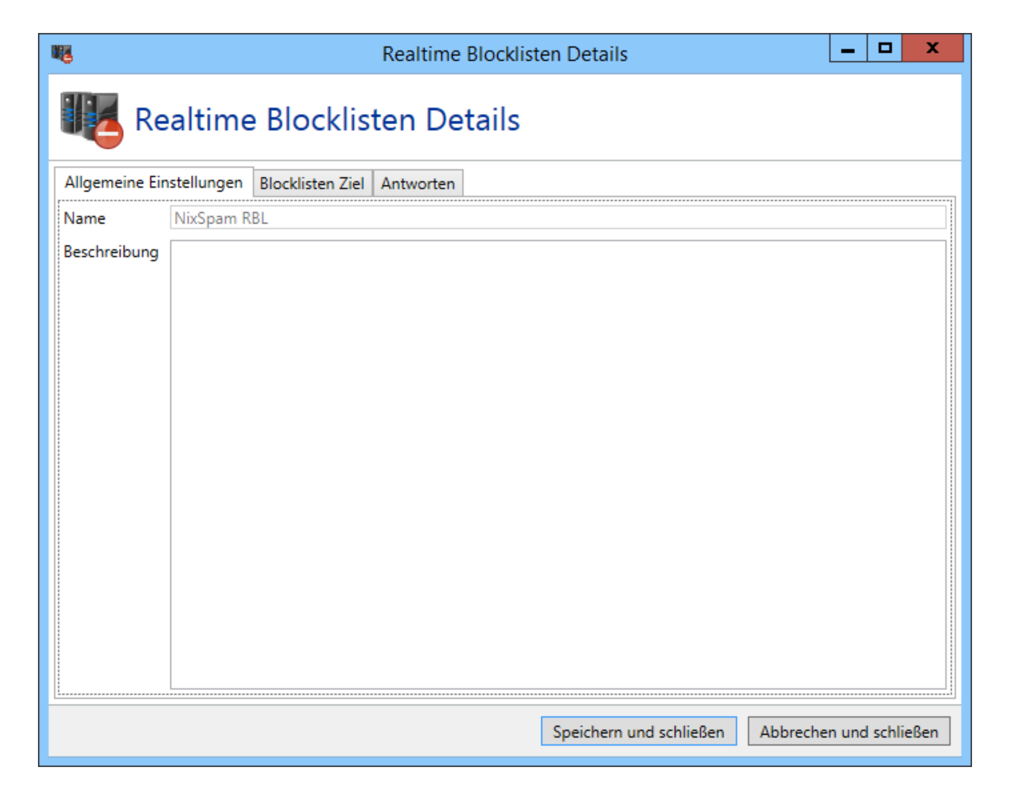


Bild 105: Geben Sie den Namen und eine Beschreibung der Blocklist ein

Auf der Registerkarte **Blocklist-Ziel** geben Sie an, ob es sich um eine RBL-Liste handelt, die per DNS oder HTTP angesprochen wird. Im Feld **Adresse** wird dann entweder die IP-Adresse oder der Servername des abzufragenden Servers eingetragen.

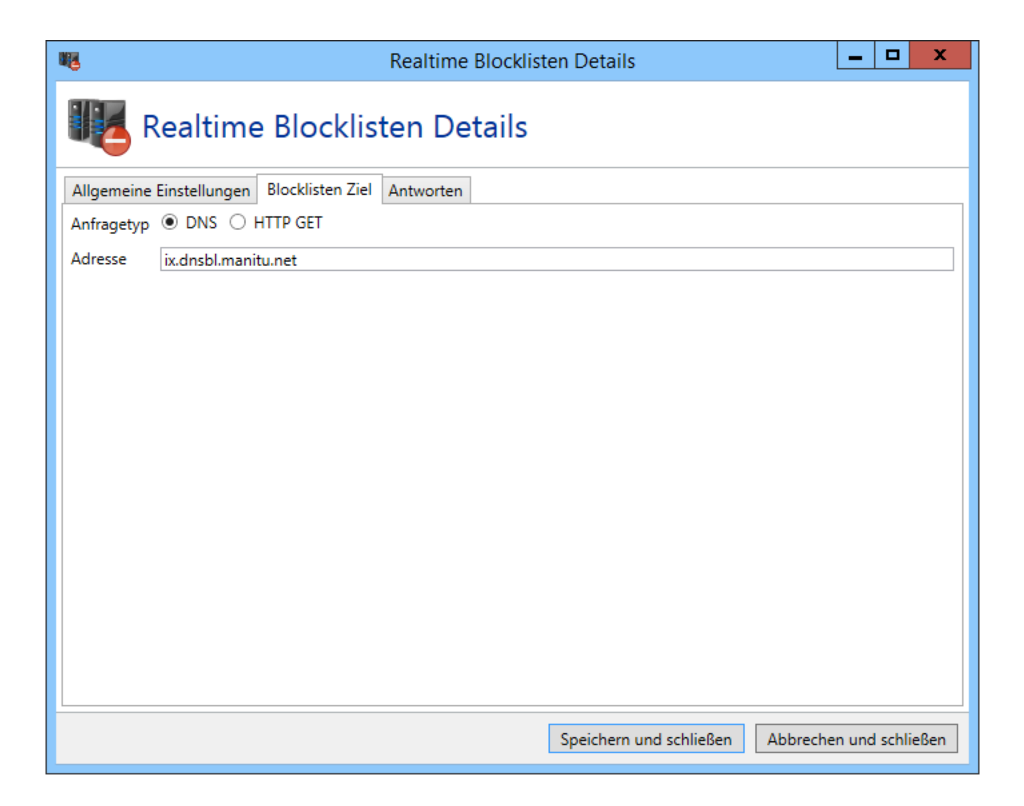


Bild 106: Der Dialog für die Definition einer Blocklist-Antwort

Auf der Registerkarte **Antworten** definiert man die möglichen Antworten des angefragten Servers und deren Bedeutung (Bild 107).

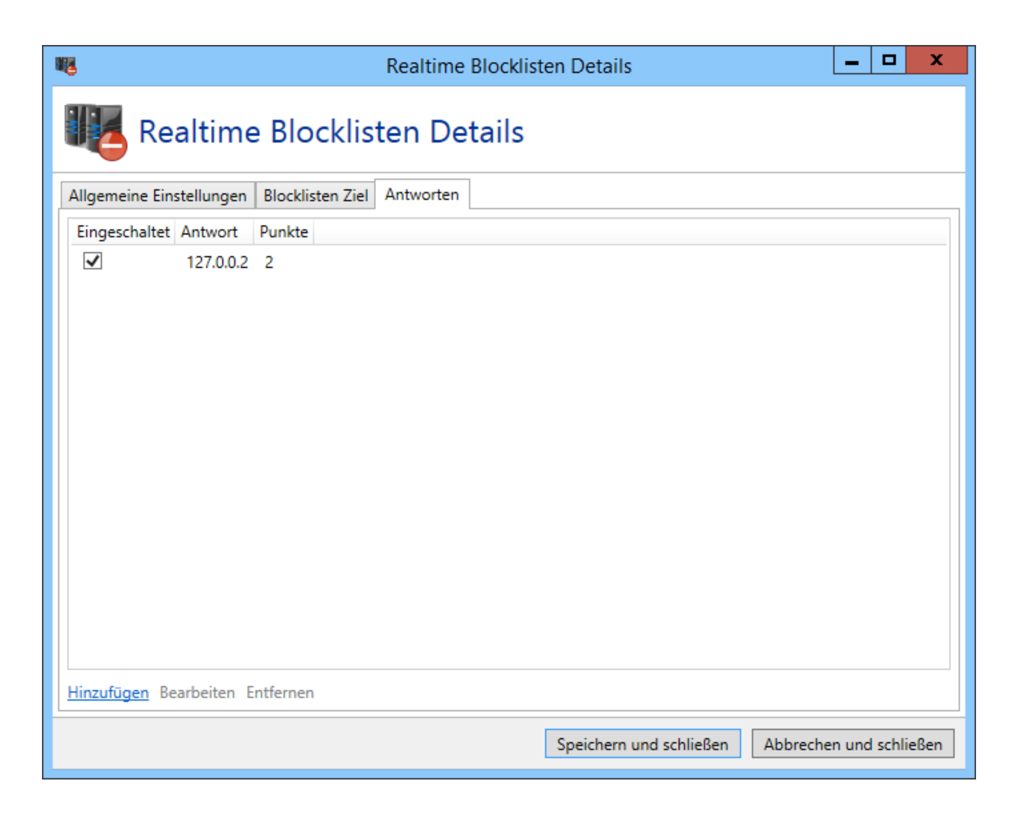


Bild 107: Alle zu erwartenden Antworten der Blocklist und deren Bewertung in SCL Punkten

Sie können neue Antworten im Dialog **Antwort Details** (Bild 108) hinzufügen. Legen Sie für dort die Antwort fest, wieviel SCL-Punkte diese bedeutet, (ein negativer Wert entspricht Bonuspunkten, ein positiver Wert entspricht Malus Punkten,) und einen beschreibenden Fehlertext. Dieser Text taucht ggfs. im Unzustellbarkeitsbericht auf, wenn der erstellende Server dies unterstützt. So weiß der Versender der abgewiesenen E-Mail, auf welcher Blacklist er aus welchem Grund steht. Die Antwort kann in diesem Dialog auch deaktiviert werden.

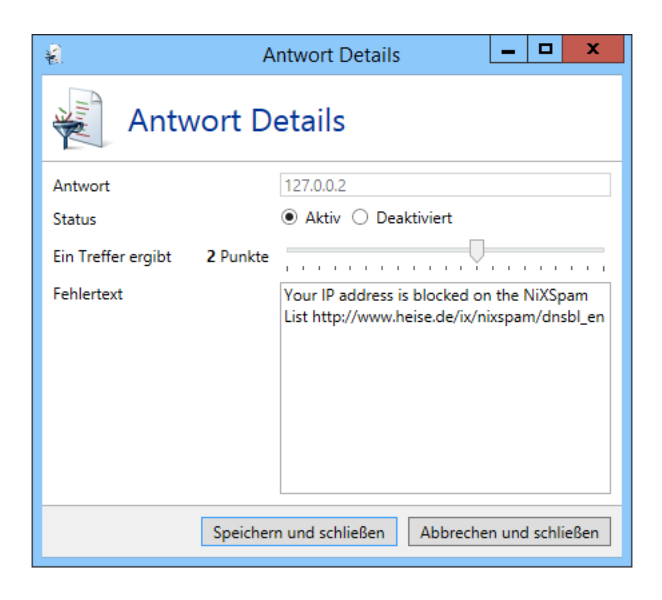


Bild 108: Eine Antwort der Liste

Wortübereinstimmungen

Im Abschnitt **Wortübereinstimmungen** haben Sie die Möglichkeit, Listen mit Ausdrücken zu pflegen, für die Sie entweder Bonus- oder Malus Punkte vergeben möchten. Die Ausdrücke werden in einzelnen Wortgruppen zusammengefasst, die Sie dann später in den einzelnen Regeln verwenden können. Pro Wortgruppe legen Sie fest, ob für die Begriffe dann Bonus- oder Malus Punkte vergeben werden soll. So haben Sie die Möglichkeit, Gruppen mit gewollten Ausdrücken und ungewollten Ausdrücken zu erstellen.

Neue Wortgruppe hinzufügen

Beim Hinzufügen einer Wortgruppe öffnet sich der Dialog **Inhalt der Wortgruppe** (Bild 109).

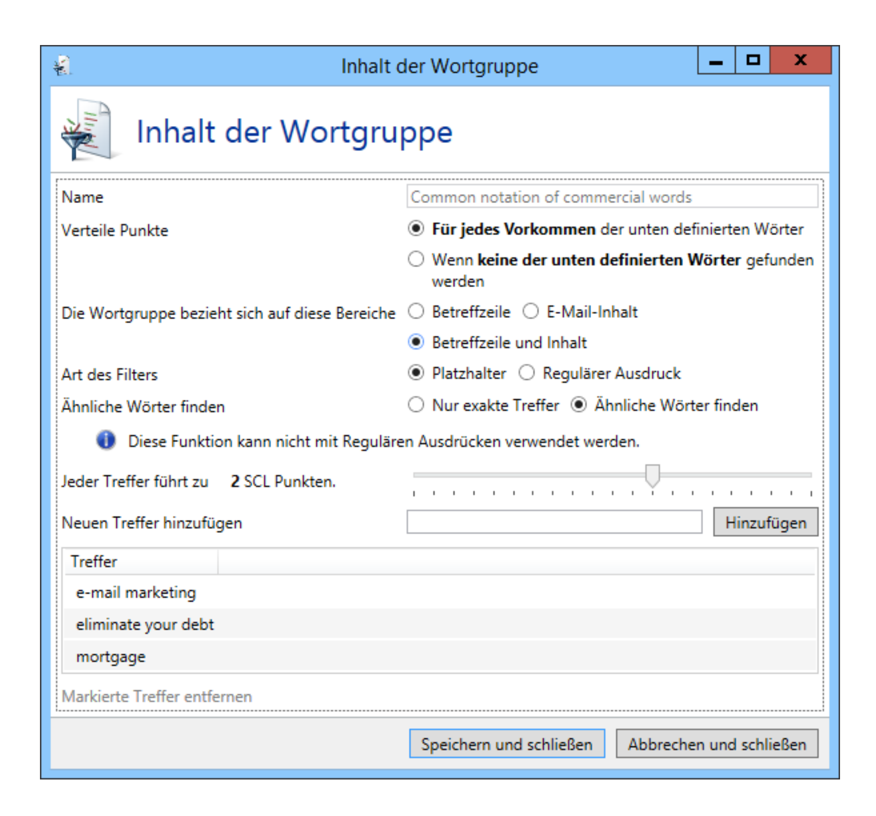


Bild 109: Definition der Wortgruppe

Als **Name** wählen Sie einen sprechenden Namen, damit Sie hinterher auch noch wissen, welche Begriffe diese Gruppe enthält.

Für jede Wortgruppe können Sie festlegen, in welchem Teil der E-Mail nach den konfigurierten Ausdrücken gesucht werden soll. Sie haben drei Auswahlmöglichkeiten. Wählen Sie **Betreffzeile** aus, wenn NoSpamProxy nach den Ausdrücken dieser Gruppe nur in der Betreffzeile einer E-Mail suchen soll. Wenn Sie die Ausdrücke im Body der E-Mail suchen lassen möchten, wählen Sie hier **E-Mail-Inhalt** aus. Alternativ können Sie auch in beiden Teilen der E-Mail die Ausdrücke suchen lassen. Wählen Sie dazu **Betreffzeile und Inhalt** aus. Dies ist auch die empfohlene Einstellung.

Zusätzlich können Sie noch einstellen, ob Sie Punkte für jedes Vorkommen eines Wortes verteilen möchten, oder ob Sie nur Punkte verteilen, wenn keins der Wörter in Inhalt oder dem Betreff zu finden ist (**Gebe Punkte**).

Sie können in den Wortgruppen zwei unterschiedliche Arten von Ausdrücken verwenden. Mit der Einstellung **Art des Filters** können Sie bestimmen, ob es sich um sogenannte Platzhalter oder Reguläre Ausdrücke handelt. Wenn Sie einfach eine Liste mit gewöhnlichem Inhalt wie zum Beispiel Viagra, Cialis, etc. anlegen möchten, wählen Sie die Option **Platzhalter** aus. Sie haben hier auch die Möglichkeit mit Platzhaltern ('*' und '?') zu arbeiten, so dass Sie auch Cialis* eingeben können, um nach allen Begriffen zu suchen, in denen das Wort Cialis am Anfang steht.

Wenn Sie bereits fertige Reguläre Ausdrücke erstellt haben, können Sie diese auch weiterhin verwenden. Dazu wählen Sie bei der Einstellung **Art des Filters** die Option **Regulärer Ausdruck**.

Die Einstellung **Ähnliche Wörter finden** steht Ihnen nur zur Verfügung, wenn Sie in der Einstellung **Art des Filters** die Option **Platzhalter** ausgewählt haben. Sie können dann bestimmen, ob NoSpamProxy nur nach exakt den angegebenen Begriffen oder auch nach ähnlichen Wörtern suchen soll. Wählen Sie die Option **Nur exakte Treffer** und geben bei den Treffern das Wort Viagra an, wird NoSpamProxy auch nur nach dem Wort Viagra suchen. Die Suche ist nicht case sensitive, so dass die Groß- und Kleinschreibung zu vernachlässigen ist. Aber die Variante V1agr@ wird NoSpamProxy mit dieser Einstellung nicht finden. Wählen Sie hingegen die Option **Ähnliche Wörter finden**, macht NoSpamProxy aus dem Wort Viagra automatisch einen Regulären Ausdruck und erkennt damit auch ähnliche Schreibweisen, wie zum Beispiel Vlagra, \/1@gra oder V-I-A-G-R-A.

Mit dem Schieberegler **Neuen Treffer hinzufügen** legen Sie fest, wie viele Malus- oder Bonuspunkte pro Treffer vergeben werden sollen. Sie können Werte zwischen -10 und 10 einstellen. Der Wert -10 entspricht hier Bonuspunkten. Die Einstellung 10 entspricht dann 10 Malus Punkten.



Wenn Sie Änderungen an den Wortgruppen vornehmen, wirken sich diese auf alle Regeln aus, die den Filter „Wortübereinstimmungen“ verwenden und die entsprechende Wortgruppe konfiguriert haben.

CSA-Whitelist

Um die CSA-Whitelist Aktion zu verwenden, müssen Sie zuerst den Download der Liste konfigurieren. Wählen Sie dazu **Einstellungen bearbeiten**. Es öffnet sich der Dialog für die Konfiguration (Bild 110).

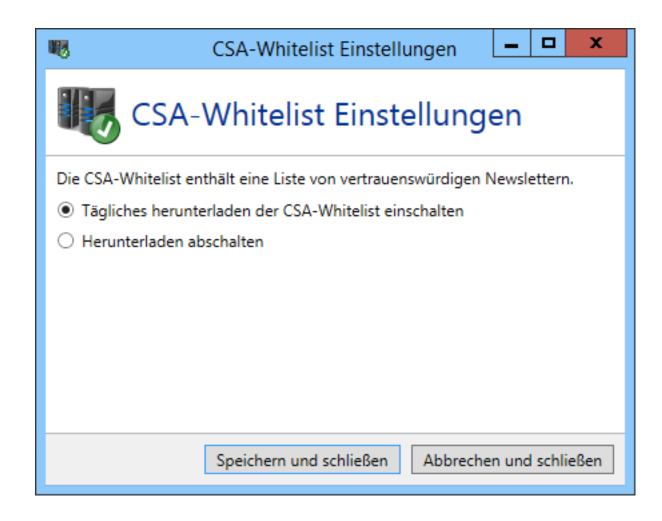


Bild 110: Konfigurieren Sie das Herunterladen der CSA-Whitelist

Wählen Sie **Tägliches herunterladen der CSA-Whitelist einschalten** wenn Sie die CSA-Whitelist Aktion verwenden wollen. Ansonsten können Sie **Herunterladen abschalten** wählen.



Die CSA-Whitelist wird von der Adresse `https://mailgateway-services.netatwork.de/1/ClientSupportService.svc` heruntergeladen. Damit Ihr Mail Gateway diese Liste laden kann, benötigt es den Zugriff auf diese Adresse. Bitte schalten Sie ggf. Ihre Firewall dafür frei.

Gateway Komponenten

Unter dem Menüpunkt **Gateway Komponenten** werden die Verbindungen zwischen den einzelnen Komponenten des Mail Gateway konfiguriert (Bild 111).

Bild 111: Die Verbindungen zu einzelnen Komponenten des Mail Gateways

Gateway Rollen

Die Intranet Rolle kann entweder auf demselben Server wie die Gateway Rolle installiert werden oder aber auf einem anderen Server.



Die Konfiguration wird von der Intranet Rolle zu allen verbundenen Gateway Rollen übertragen. Falls Sie in Ihrem Unternehmen eine DMZ betreiben, sollten Sie die Gateway Rollen dort, die Intranet Rolle aber im internen Netz installieren. In Ihrer Firewall brauchen Sie dann nur die Verbindung vom internen Netz zur DMZ für die TCP-Ports 6060 und 6061 freischalten.

Server-Identität

Bei einer ausgehenden Verbindung, stellt sich der Client mit dem HELO oder EHLO Kommando gefolgt vom Servernamen beim empfangenen Server vor. Ein mögliches Beispiel:

```
EHLO gate.netatwork.de
```

Einige Server überprüfen, ob dieser Name per DNS auflösbar ist. Die Auflösbarkeit dieses Namens ist in einer RFC vorgeschrieben. Sollte der Name nicht auflösbar sein, wird das von einigen anderen Mail Servern als Spam-Merkmal bewertet. Hier sollte der im Internet auflösbare FQDN eingetragen werden. Üblicherweise wird hier der MX der eigenen E-Mail-Domäne eingetragen.

Um die genannte Einstellung zu ändern, klicken Sie im Bereich **Server-Identität** auf **Ändern**. Es erscheint der Dialog zum Ändern der Identität (Bild 112).

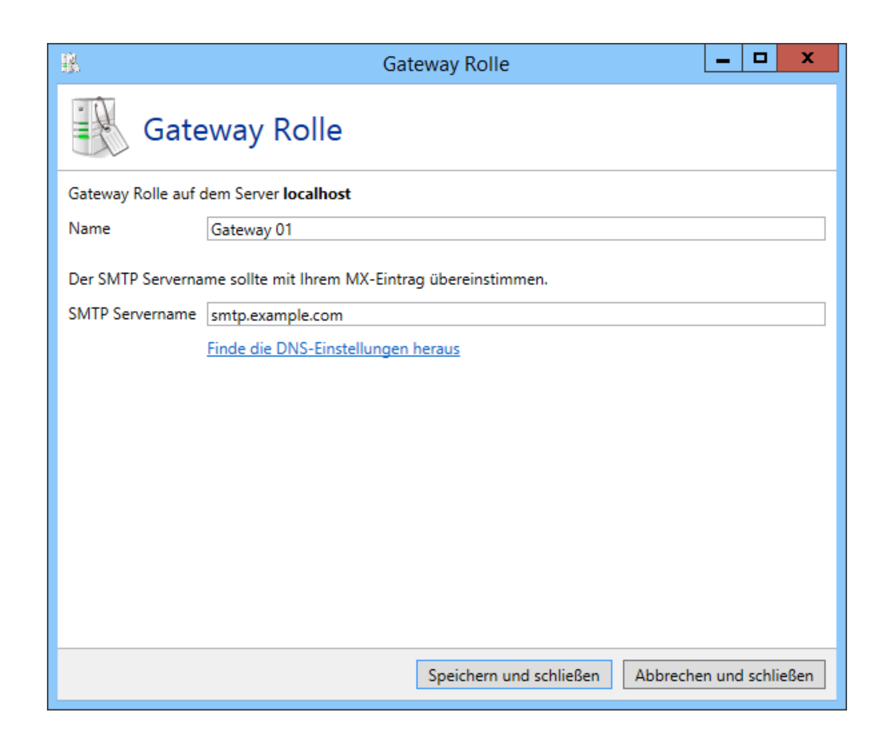


Bild 112: Die Server-Identität sollte dem „MX“ Eintrag in Ihrem DNS entsprechen

Im Feld **Name** geben Sie dann den zu verwendenden Namen an.

Sie können auch den DNS Namen für Ihre Domäne automatisch auflösen lassen. Dazu wird die primäre Domäne Ihrer Lizenz benutzt. Für die automatische Auflösung drücken Sie den Knopf **Externe DNS Identitäten ermitteln**. Es erscheint ein Dialog, der alle zur Verfügung stehenden DNS Identitäten für Ihre Domäne, nach der Priorität geordnet, auflistet.

Verbindung zu einer Gateway Rolle herstellen

Im Dialog für die Verbindung zu einer Gateway Rolle (Bild 113) wählen Sie die Option **Die Rolle und die Gateway Rolle laufen beide auf demselben Server**, wenn Sie die zu verbindenden Rollen auf dem gleichen Server installiert haben. Ist die Gateway Rolle auf einem anderen Server installiert, wählen Sie zunächst die Option **Die Rolle und die Gateway Rolle laufen auf unterschiedlichen Servern...** Geben Sie dann unter **Servername** und **Port** den Namen der Gateway Rolle an, unter dem die aktuelle Rolle die Gateway Rolle erreichen kann. Wenn die Management Rolle sich zur Gateway Rolle mit denselben Daten verbinden kann, wählen Sie die Option **Die Management Konsole kann sich zur Gateway Rolle mit dem oben angegeben Servernamen und Port verbinden**. Ansonsten wählen Sie **Die Management Konsole kann sich zur Gateway Rolle mit dem unten angegeben Servernamen und Port verbinden** und geben Sie dann die Daten in das Feld **Servername** und **Port** ein. Standardmäßig ist der Port 6060.

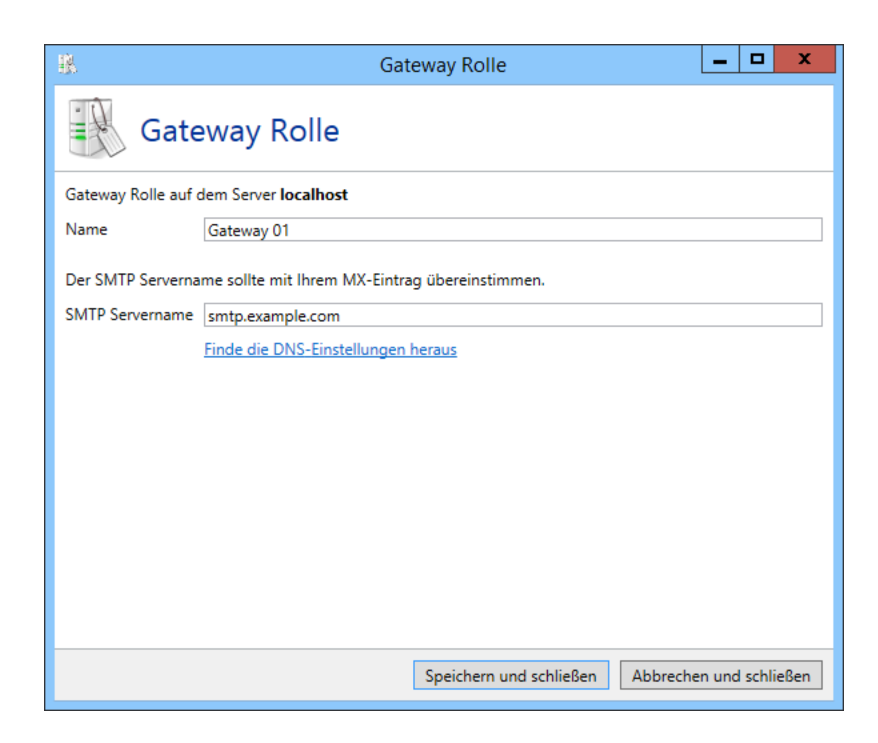


Bild 113: Die Einstellungen für eine Verbindung zu einer Gateway Rolle

Web Portal

Um das Web Portal verwenden zu können, müssen Sie zunächst eine Verbindung von der Intranet Rolle zum Web Portal herstellen. Anschließend können Sie die einzelnen Features konfigurieren.



Das Web Portal steht Ihnen nur zu Verfügung, wenn Sie den Large File Transfer lizenziert haben.

Im Dialog für eine Verbindung zum Web Portal (Bild 114) geben Sie unter **Adresse** die HTTPS-Adresse des Web Portals, zum Beispiel: `https://portal.example.com/` oder `https://portal.example.com:1234/` für eine Verbindung über den Port '1234', unter dem die Intranet Rolle das Web Portal erreichen kann. Wenn die Management Rolle sich zur Gateway Rolle mit denselben Daten verbinden kann, wählen Sie die Option **Die Management Konsole kann sich über die oben angegebenen Adresse mit dem Web Portal verbinden**, ansonsten wählen Sie **Die Management Konsole kann sich über die unten angegebenen Adresse mit dem Web Portal verbinden** und geben Sie die HTTP-Adresse in das Feld **Adresse** ein, unter der die Management Konsole das Web Portal erreichen kann. Standardmäßig ist das der Port 443.

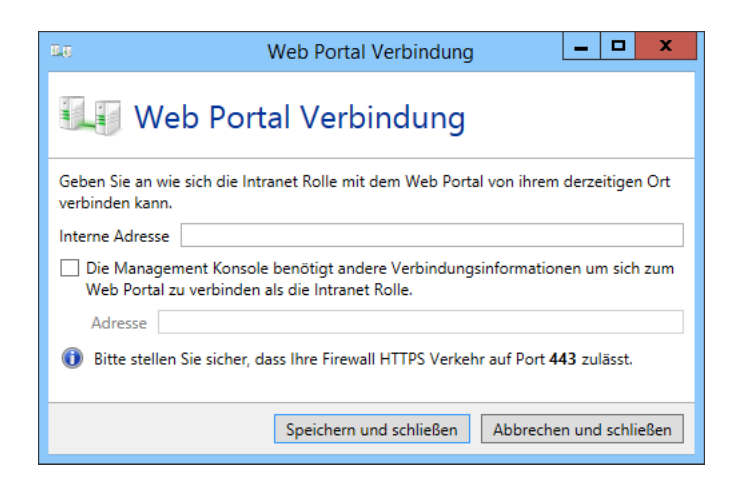


Bild 114: Die Einstellungen für eine Verbindung zu einem Web Portal

Bei Benutzung des Web Portals wird in ausgehende Mails ggf. ein Link auf das Web Portal eingefügt. Der Link beinhaltet dabei die Adresse unter der das Web Portal aus dem Internet erreichbar ist (Bild 115).

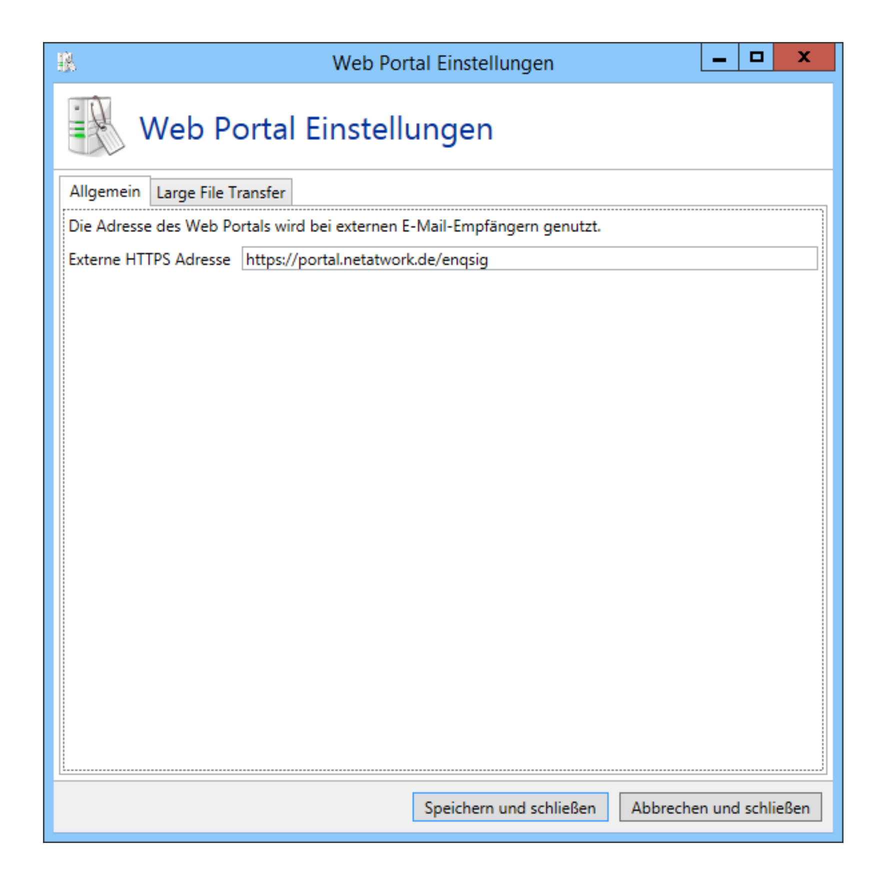


Bild 115: Allgemeine Einstellungen

Wenn Sie den Large File Transfer aktivieren, müssen Sie auf der nächsten Seite noch einige weitere Einstellungen vornehmen (Bild 116). Um die Kommunikation zwischen dem Outlook Add-In und dem Web Portal abzusichern ist ein Passwort ("Shared Secret") notwendig. Geben Sie ein Kennwort ein, dass mindestens 12 Zeichen lang ist.

Falls Sie die Daten des Large File Transfers an einem anderen Ort speichern möchten, so können Sie das neue Verzeichnis unter **Speichere Daten unter** angeben. Die Daten werden nach Ablauf der Speicherfrist (**Entferne Dateien nach x Tagen**) vom Web Portal entfernt und stehen dann nicht mehr zum Herunterladen zur Verfügung.

Mit NoSpamProxy können alle Dateien im Large File Transfer mit dem **CYREN-Antivirus-Dienst** überprüft werden.

Des Weiteren können Sie hier noch einige Schwellwerte festlegen: Mit dem ersten Schieber legen Sie fest, ab wann der Large File Transfer zum Einsatz kommt. Anhänge, die kleiner sind, werden bei Antworten direkt an die E-Mail angehängt; größere werden über den Large File Transfer übermittelt. Zusätzlich können Sie die maximale Größe für angehängte Dateien beschränken, sowie die Maximalgröße für alle Anhänge festlegen.



Die Schwellwerte für die maximale Dateigröße sowie dem Limit für die Größe aller Anhänge gelten auch für das Outlook Add-In; der Schwellwert, der festlegt, ob der Large File Transfer verwendet wird, gilt nur für Antworten über das Web Portal.

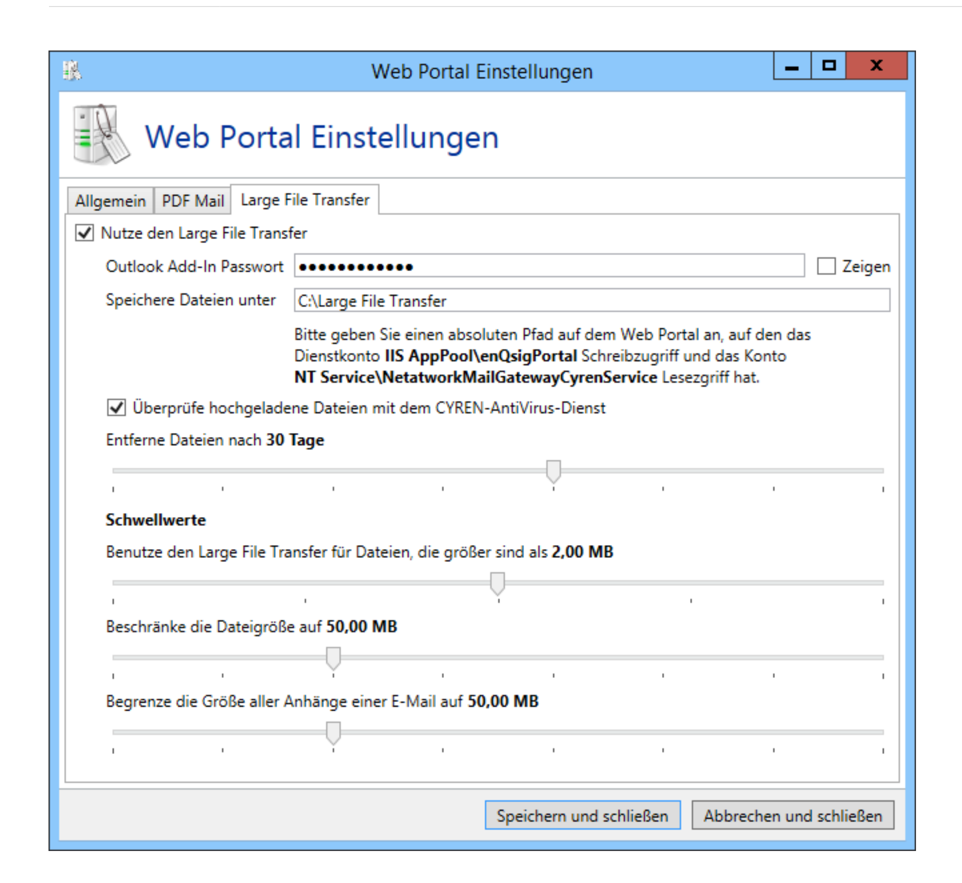


Bild 116: Einstellungen für den Large File Transfer

Datenbanken

Im Bereich der **Datenbankkonfiguration** können Sie die Verbindung zur Datenbank der entsprechenden Rolle ändern. Die Datenbank wird während des Setups eingerichtet. Änderungen müssen nur im Falle eines Umzugs der Datenbank auf einen anderen SQL-Server vorgenommen werden. In einem solchen Fall sollten Sie die bestehende Datenbank auf dem bisherigen SQL Server sichern und diese Sicherung auf dem neuen Datenbank Server einspielen. Stellen Sie nun die Verbindung auf den neuen Datenbank Server mit **Datenbankkonfiguration ändern** um (Bild 117).

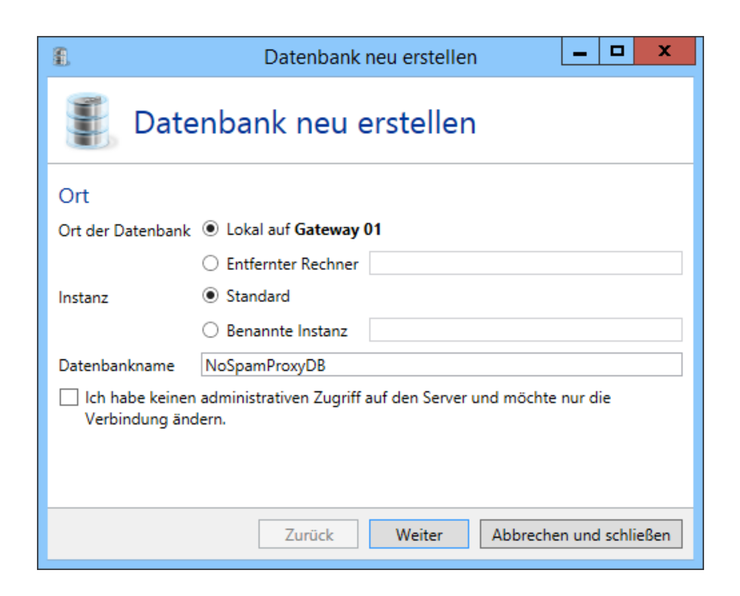


Bild 117: Die Verbindung zur Datenbank der entsprechenden Rolle

Mit der Einstellung **Ort der Datenbank** bestimmen Sie, auf welchem Server sich die Datenbank befindet. Wenn sich die Datenbank auf demselben Server wie die Gateway Rolle befindet, wählen Sie **Lokaler Server**. Ist die Datenbank auf einem anderen Server eingerichtet, wählen Sie zunächst die Option **Entfernter Server** und geben dann im Feld **Entfernter Servername** entweder die IP-Adresse oder den voll qualifizierten Domänennamen (FQDN) des Servers ein, auf dem sich die Datenbank befindet.

Ob es sich bei der Instanz, in der die Datenbank der Gateway Rolle liegt, um die Standardinstanz des SQL-Servers oder um eine benannte Instanz handelt, geben Sie mit **Datenbank Instanz** an. Wenn es sich um die Standardinstanz des SQL-Servers handelt, wählen Sie die Option **Standardinstanz**. Anderenfalls klicken Sie auf **Benannte Instanz** und tragen anschließend im Feld **Instanzname** den Namen der entsprechenden Instanz ein.

In dem Feld **Datenbankname** bzw. den Feldern, wenn mehrere Datenbanken für die Rolle benötigt werden, tragen Sie den Namen der entsprechenden Datenbank ein. Die folgenden Datenbanknamen werden standardmäßig verwendet.

- **Gateway Rolle**
  `NoSpamProxyDb`
- **Intranet Rolle**
  `NoSpamProxyAddressSynchronization`

Wenn Sie lediglich die Verbindungsparameter ändern möchten, markieren Sie das entsprechende Feld im unteren Bereich des Dialogs.

Die Einstellung **Administrative Authentifizierung** (Bild 118) legt fest, mit welchem Benutzerkonto Änderungen an der gewählten Datenbank durchgeführt werden sollen. Wählen Sie die Einstellung **Windows**, wenn Sie ein Windows-Benutzerkonto verwenden möchten. Andernfalls wählen Sie die

Option **SQL Server** und tragen anschließend in den Feldern **Benutzername** und **Passwort** die entsprechenden Anmeldedaten ein.

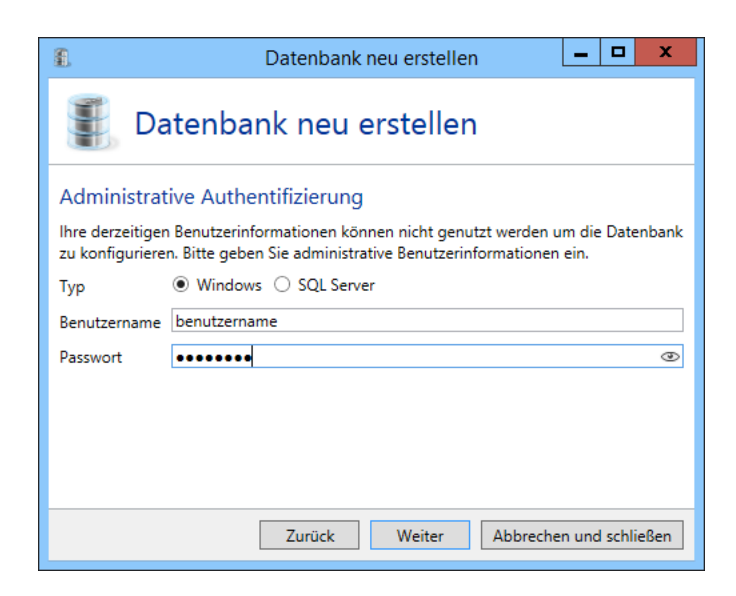


Bild 118: Die Verbindung zur Datenbank der entsprechenden Rolle

Die Einstellung **Service Authentifizierung** (Bild 119) legt fest, wie sich die Gateway Rolle beim SQL Server anmelden soll. Ist auf dem SQL-Server die SQL-Authentifizierung abgeschaltet, dann muss die integrierte Authentifizierung verwendet werden. Ansonsten können Sie hier zwischen Integrierter und SQL-Authentifizierung wählen. (Bild 120).

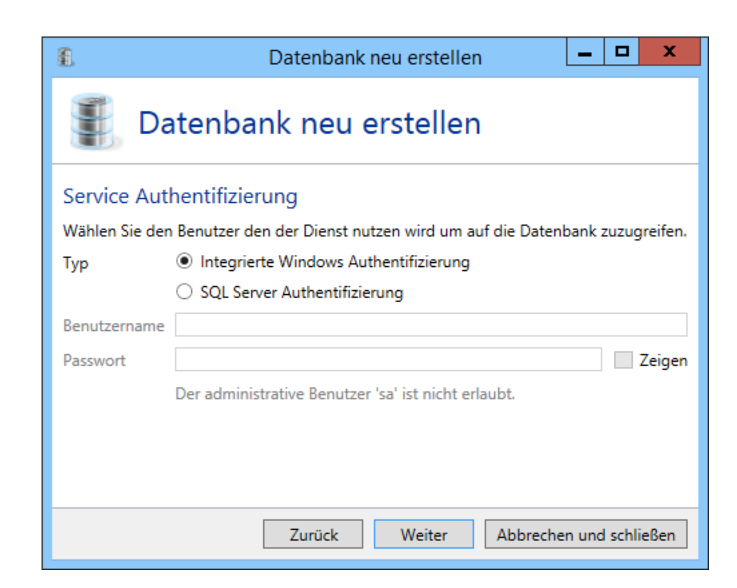


Bild 119: Dienstanbindung an die Datenbank.

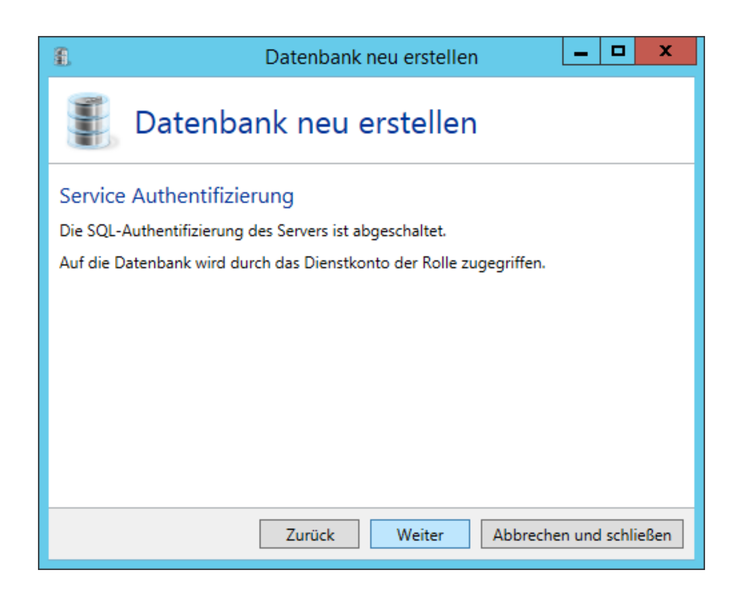


Bild 120: Keine SQL-Authentifizierung verfügbar.

Auf der Seite **Was soll getan werden** wählen Sie nun die gewünschte Aktion aus. Je nachdem, was das Mail Gateway für eine Datenbank gefunden hat, stehen hier andere Möglichkeiten zur Verfügung. Wählen Sie die gewünschte Aktion aus und klicken Sie auf **Fertigstellen** (Bild 121).

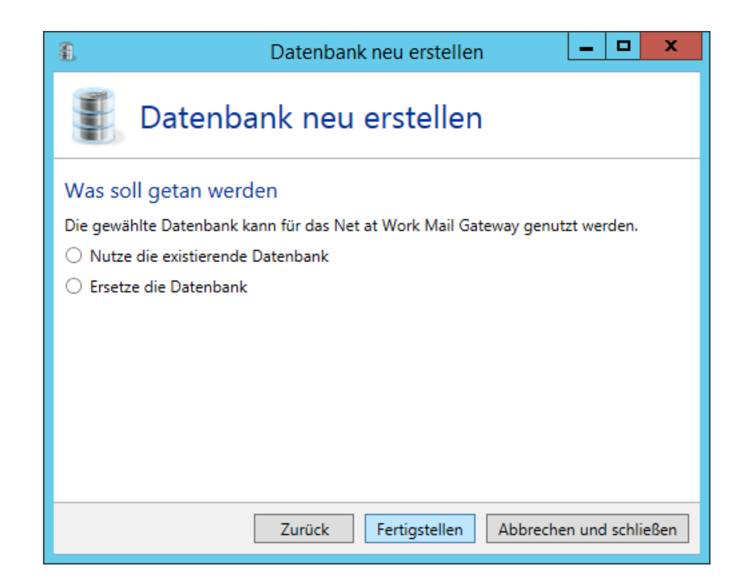


Bild 121: Wählen Sie ob die alte Datenbank gelöscht oder erhalten werden soll

Verbundene Systeme

Der Knoten **verbundenen Systeme** beinhaltet Verbindungen zu Drittanbieterprodukten die mit dem Net at Work Mail Gateway interagieren (Bild 122).

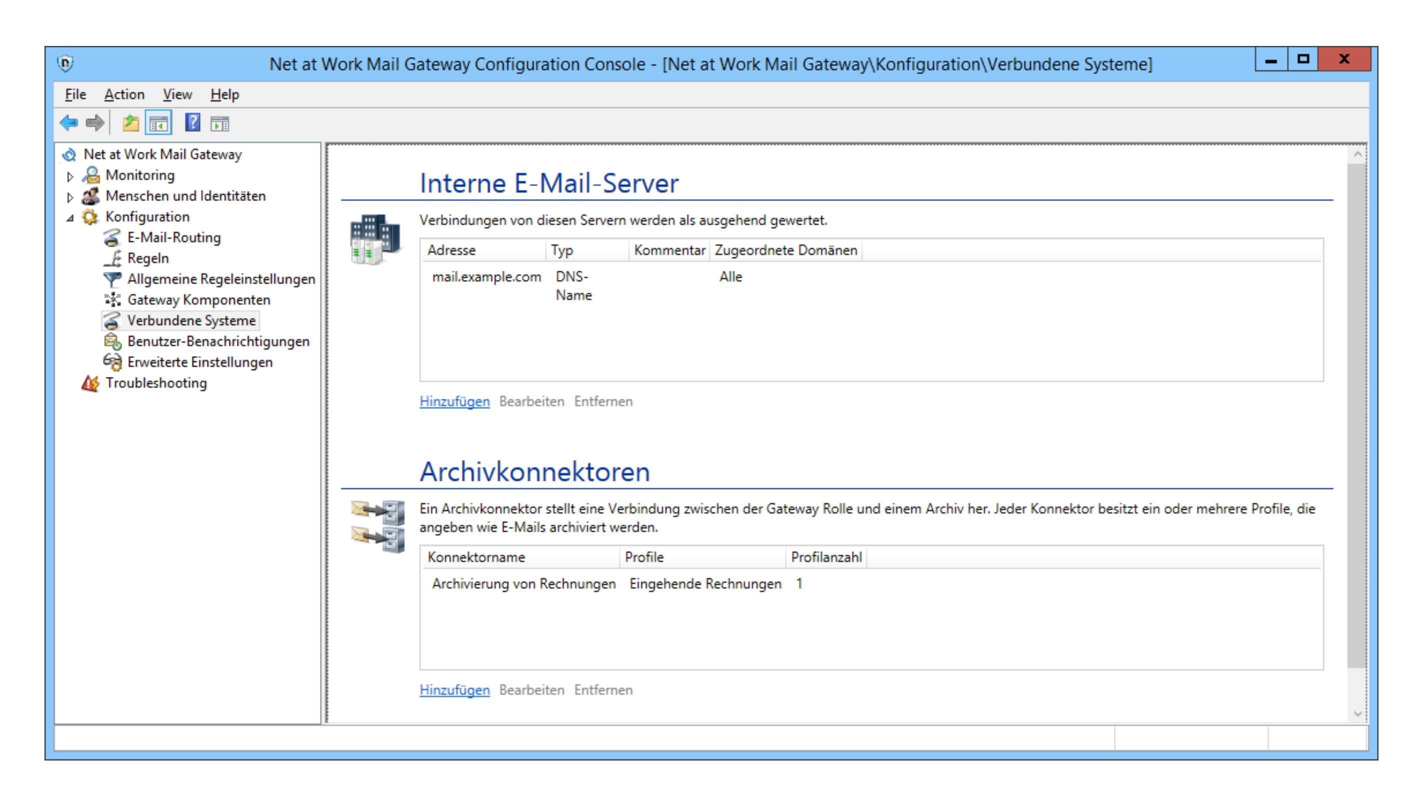


Bild 122: Hinzufügen eines internen Servers

Interne E-Mail-Server

Im Abschnitt **Interne E-Mail-Server** sind alle internen E-Mail-Server Ihres Systems anzugeben, die über das Net at Work Mail Gateway ausgehende E-Mails verschicken sollen. Nur Verbindungen von diesen E-Mail-Servern ordnet das Gateway als ausgehend ein.



Alle Client-Verbindungen sollten ausschließlich über die internen E-Mail-Server laufen, damit das Net at Work Mail Gateway alle E-Mails erfassen kann.

Beim Hinzufügen von neuen internen E-Mail-Servern tragen Sie zunächst den Namen, die IP-Adresse oder das Subnetz des hinzuzufügenden Servers ein (Bild 123). Im zweiten Schritt können Sie noch festlegen, für welche der internen Domänen der Server zuständig ist (Bild 124). Versucht ein Server später eine E-Mail mit einer Absenderdomäne zu senden, für die er nicht berechtigt ist, so wird die Zustellung abgelehnt.

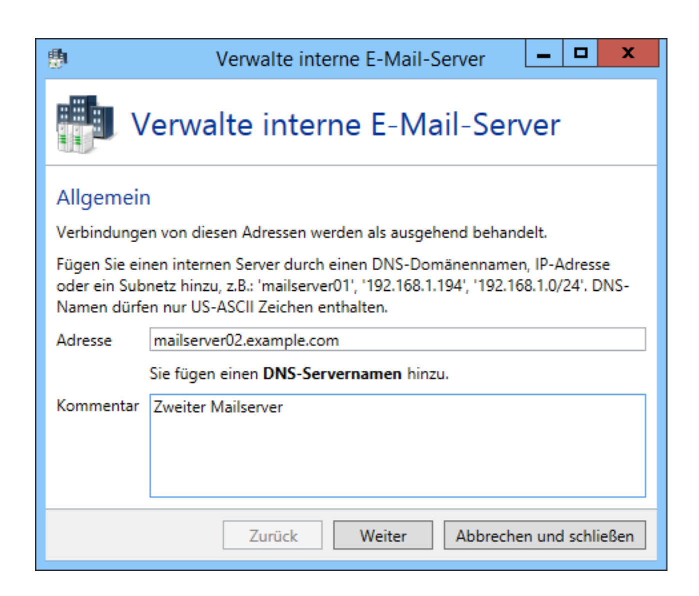


Bild 123: Allgemeine Einstellungen für neue interne Server

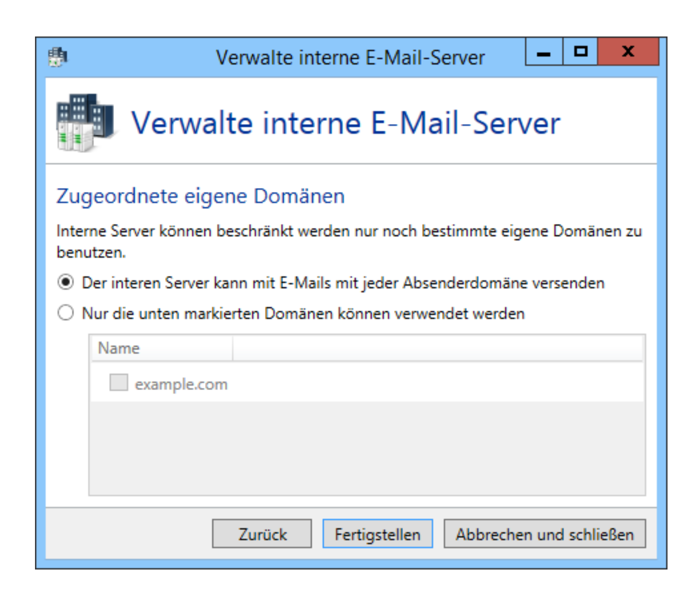


Bild 124: Domänen-Restriktion für neue interne Server

Archivschnittstelle

Über die Archivschnittstelle können E-Mails und qualifiziert signierte Dokumente an ein externes Archivsystem übergeben werden. Unterstützt werden derzeit das Dateisystem, ein Archivpostfach sowie d.velop d.3. Es können auch mehrere Archivsysteme parallel verwendet werden.

Die Konfiguration besteht aus zwei Teilen: Archivkonnektoren und Profilen. Konnektoren definieren die Schnittstelle zu einem externen Archivsystem, wie z.B. dem Dateisystem. Innerhalb eines Konnektors werden ein oder mehrere Profile erstellt. Darin können Eigenschaften wie z.B. der genaue Speicherort

für E-Mails und Dokumente festgelegt werden. Außerdem wird hier ggf. eine Zuordnung von Metadaten von E-Mails auf Metadaten des Archivsystems durchgeführt.

Um einen neuen Konnektor zu erstellen, klicken Sie auf **Neuen Konnektor hinzufügen**. Hier wählen Sie zunächst den Konnektor-Typ aus und geben dem Konnektor einen neuen Namen (Bild 125).

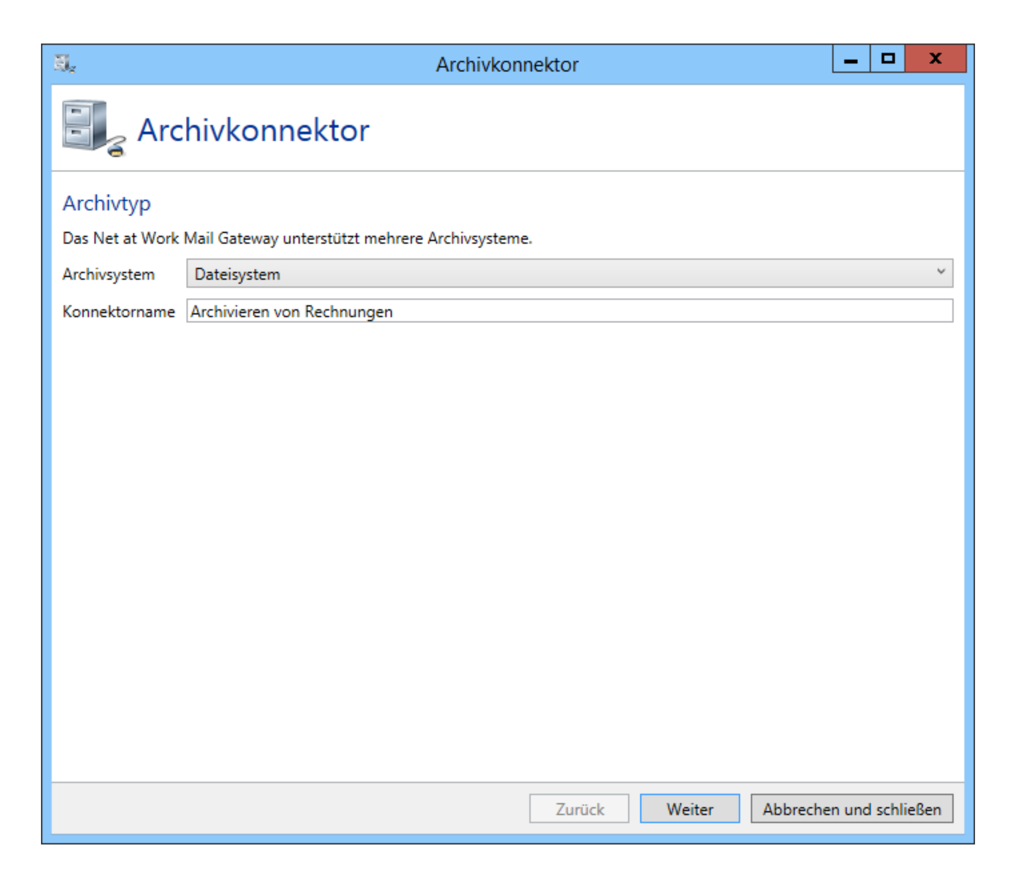


Bild 125: Allgemeine Einstellungen des Archivkonnektors

Die zu konfigurierenden Optionen im zweiten Schritt hängen davon ab, welches Archivsystem Sie im ersten Schritt gewählt haben.

Bei einer Ablage von E-Mails und Dokumenten im **Dateisystem**, ist nur ein Pfad anzugeben. E-Mails und Dokumente werden in Ordnern unterhalb dieses Pfades abgespeichert (Bild 126).

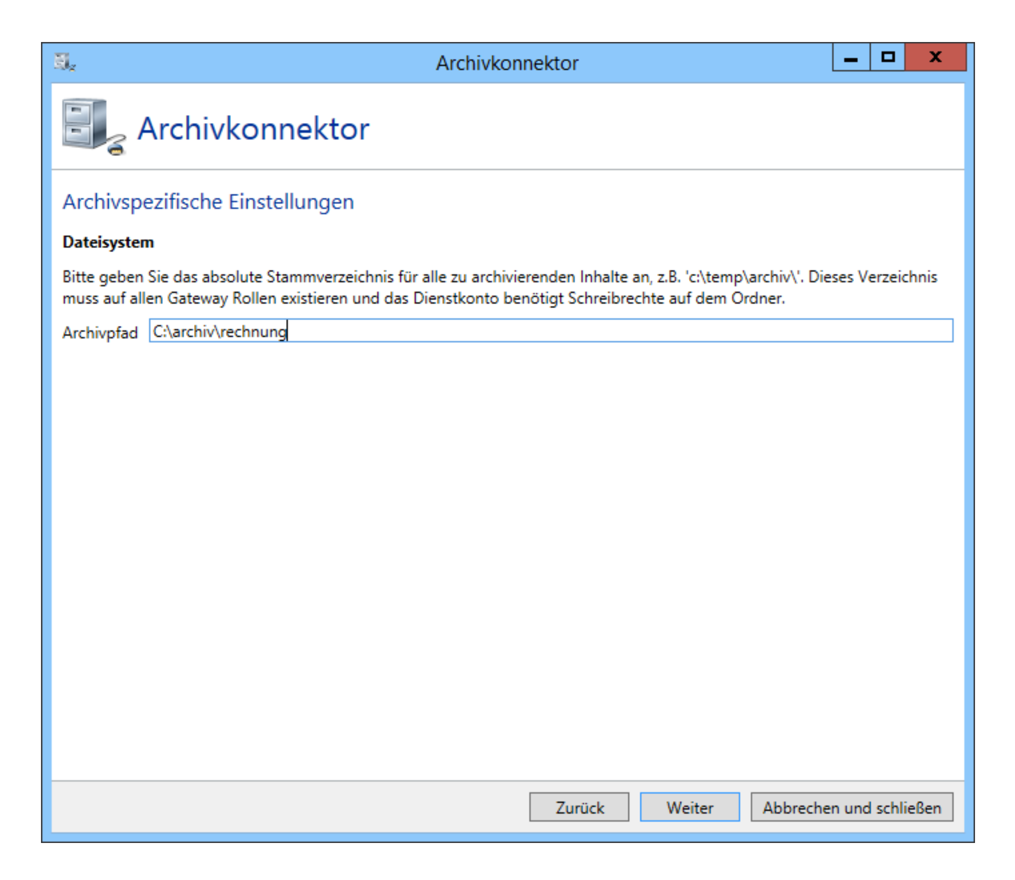


Bild 126: Eigenschaften für die Ablage im Dateisystem

Der Konnektor für das **Archivpostfach** besitzt keine weiteren Einstellungen auf dem Konnektor. Es werden direkt die Profile angezeigt.

Für einen Konnektor zu einem d.velop d.3 System ist lediglich ein Pfad anzugeben (Bild 127). E-Mails und Dokumente werden in dieses Verzeichnis geschrieben und von dort durch das d.velop d.3 System abgeholt.

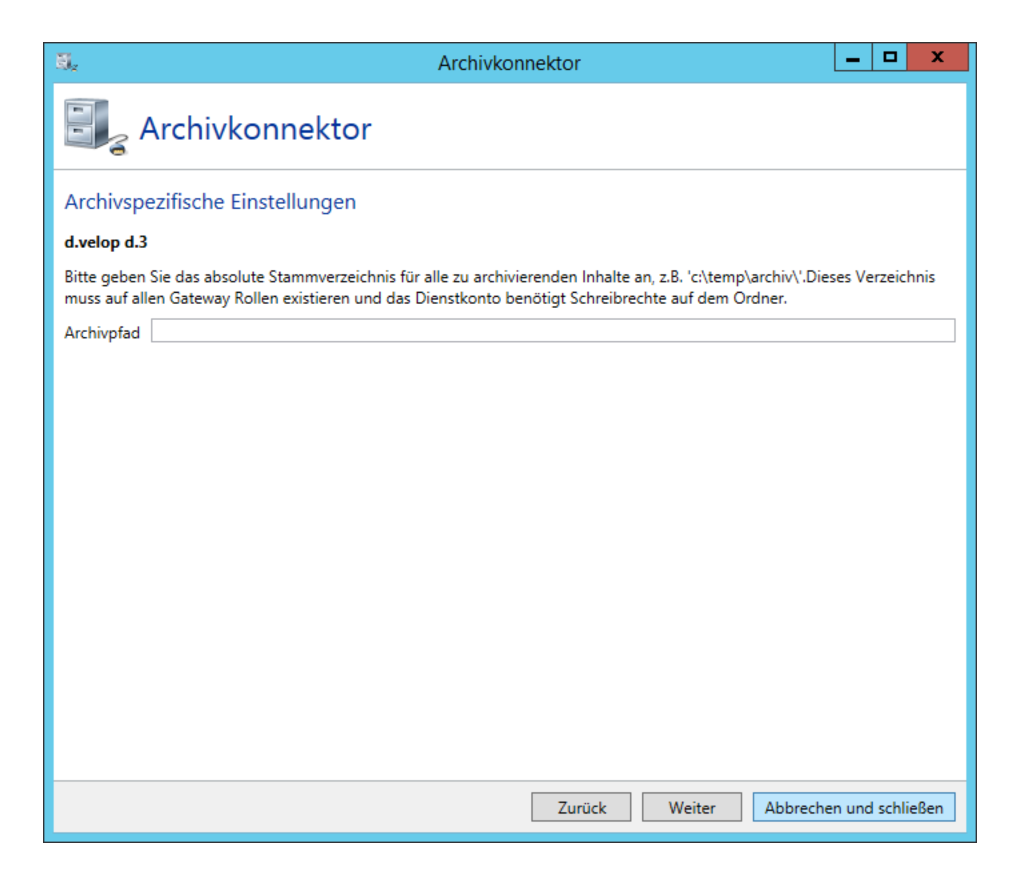


Bild 127: d.velop d.3-spezifische Eigenschaften

Auf der nächsten Seite können Sie Profile für diesen Konnektor anlegen. Profile ermöglichen es Ihnen zum Beispiel, E-Mails und Dokumente innerhalb eines Archivsystems auf verschiedene Ordner zu verteilen.

Einem neuen Profil müssen Sie zunächst einen Namen geben (Bild 128). Außerdem wählen Sie hier aus, welche E-Mails durch dieses Profil archiviert werden.

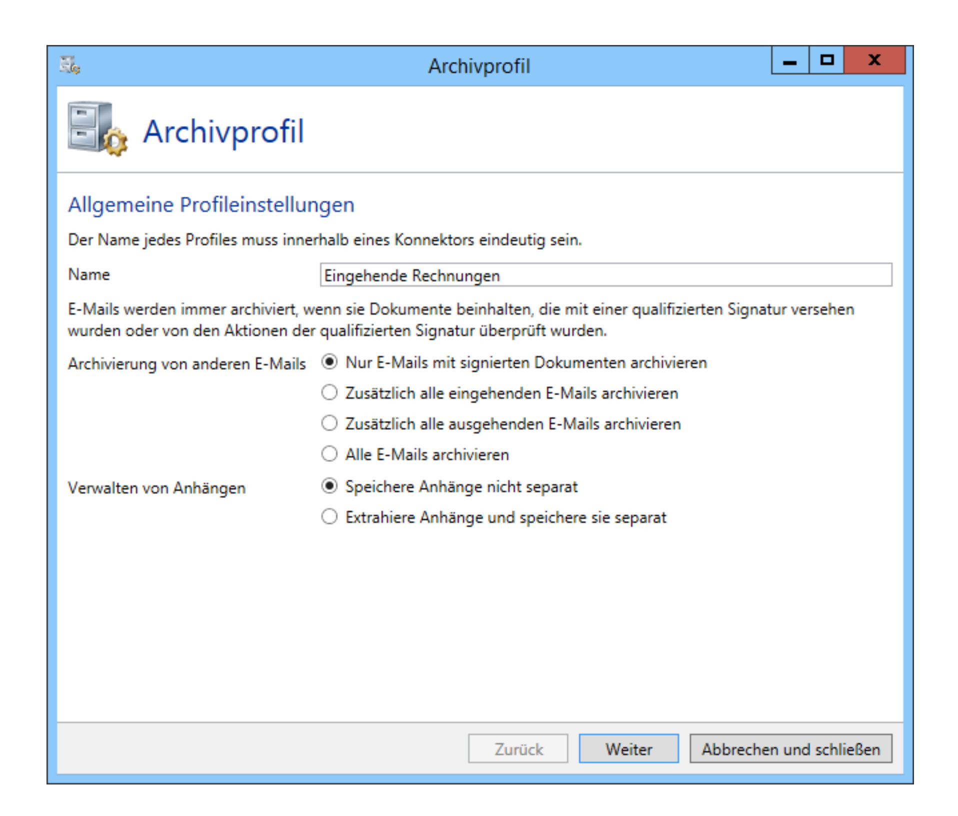


Bild 128: Allgemeine Einstellungen des Profils

Der Inhalt der zweiten Seite hängt von dem gewählten Archivsystem ab.

Für die Speicherung im **Dateisystem** können Sie einen Unterordner für die E-Mails angeben, die durch dieses Profil gespeichert werden.

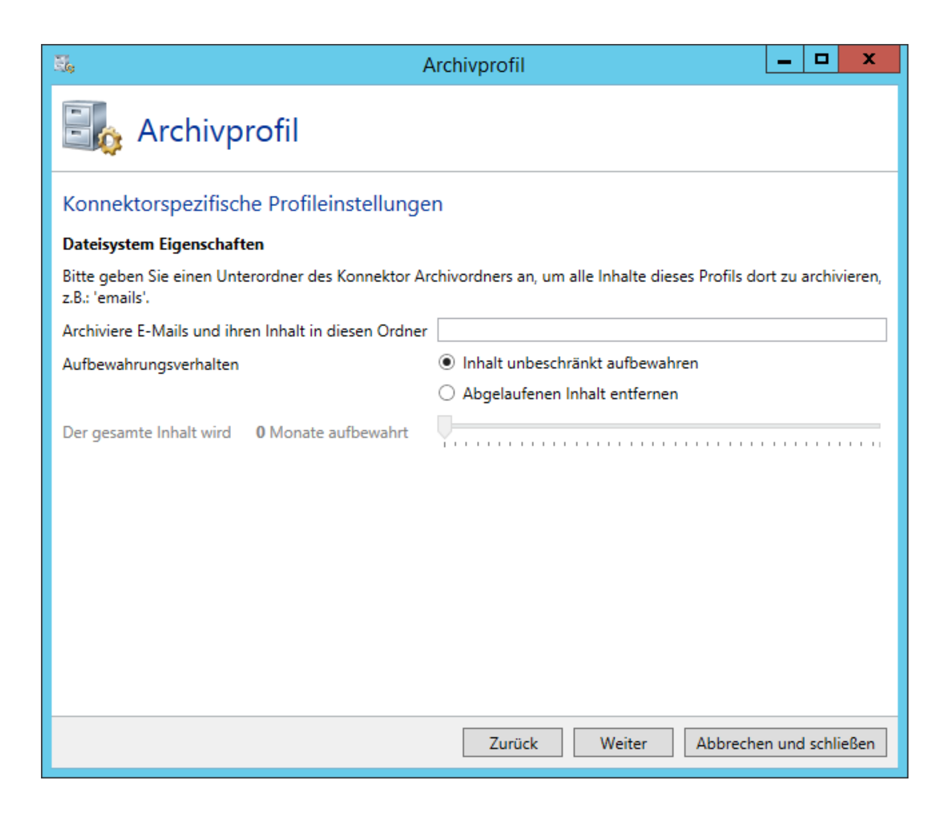


Bild 129: Eigenschaften für die Ablage im Dateisystem

Im Falle eines **Archivpostfachs** wird die E-Mail-Adresse des Zielpostfachs benötigt (Bild 130).

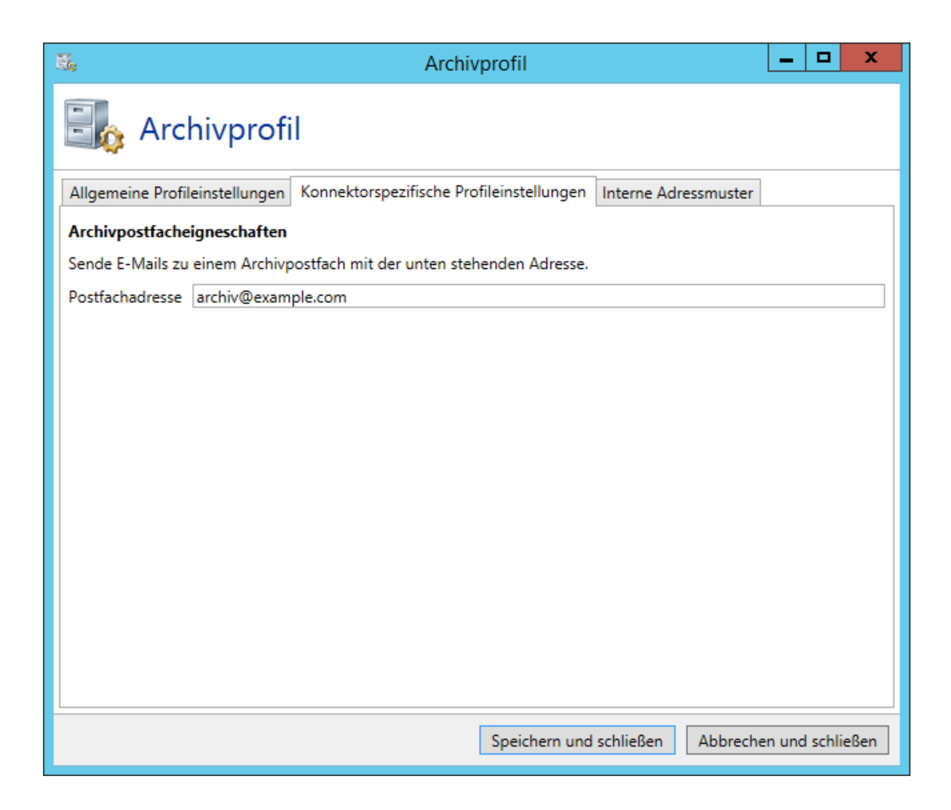


Bild 130: Eigenschaften für die Ablage in einem Archivpostfach

Bei einer Verbindung zu einem d.velop d.3 System ist keine weitere Konfiguration erforderlich. Der Dialog ist in diesem Fall leer (Bild 131).

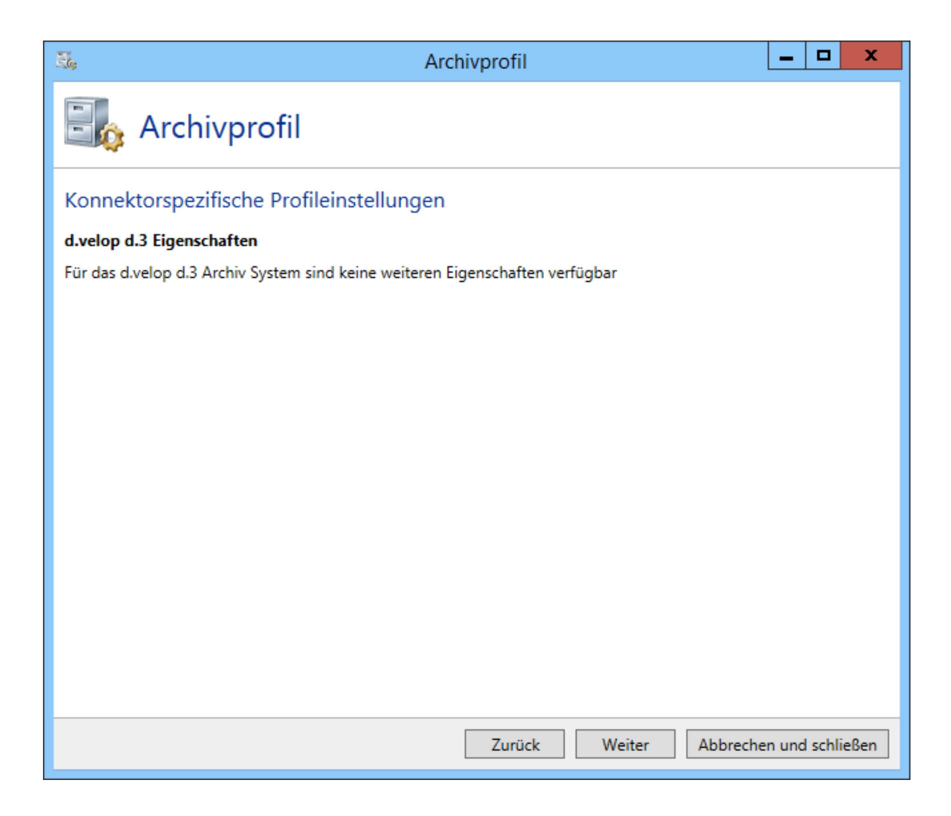


Bild 131: Eigenschaften für die Ablage in einem d.velop d.3 System

Im nächsten Schritt legen Sie fest, für welche internen E-Mailadressen dieses Profil zuständig ist. (Bild 132). Beim Versenden von ausgehenden E-Mails wird immer die Adresse des Absenders verwendet, um festzustellen, welche Profile für die Archivierung verwendet werden. Bei eingehenden E-Mails werden die Adressen der Empfänger verwendet. Bei der Angabe der E-Mail-Adressen (Bild 133) können Sie auch Platzhalter ('*' und '?') verwenden, um mehrere Adressen anzugeben. Sollten bei einem Archivierungsvorgang mehrere Profile zu den hier angegebenen Daten passen, so wird die E-Mail mehrfach archiviert.

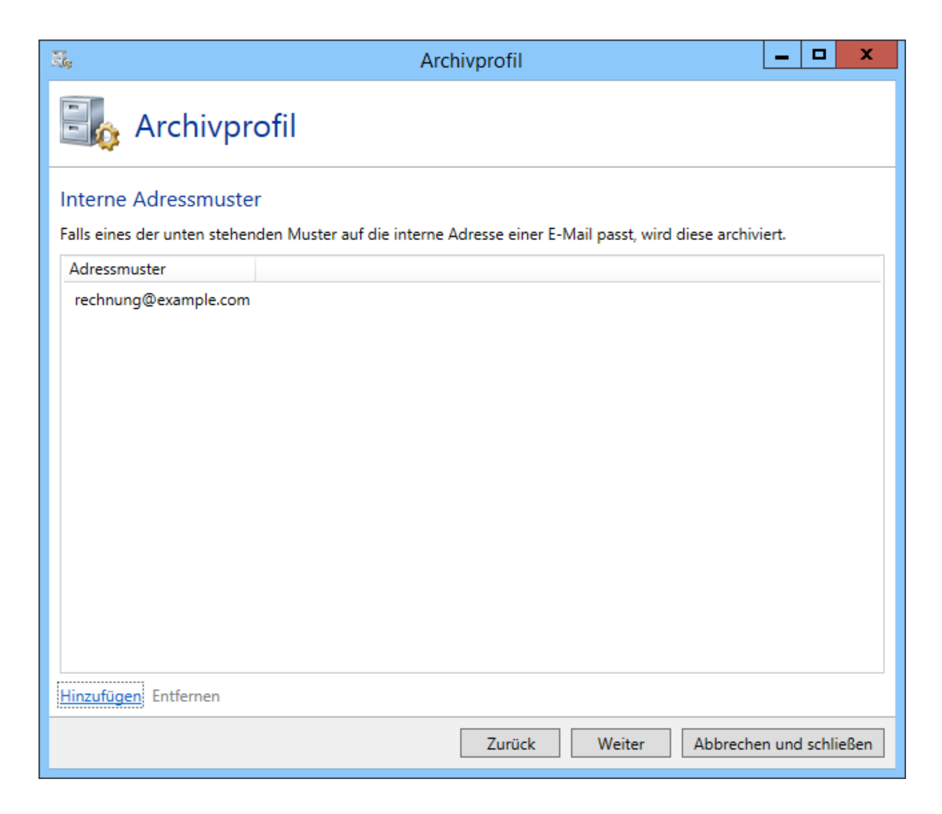


Bild 132: Zuordnung von Profilen zu internen E-Mail-Adressen

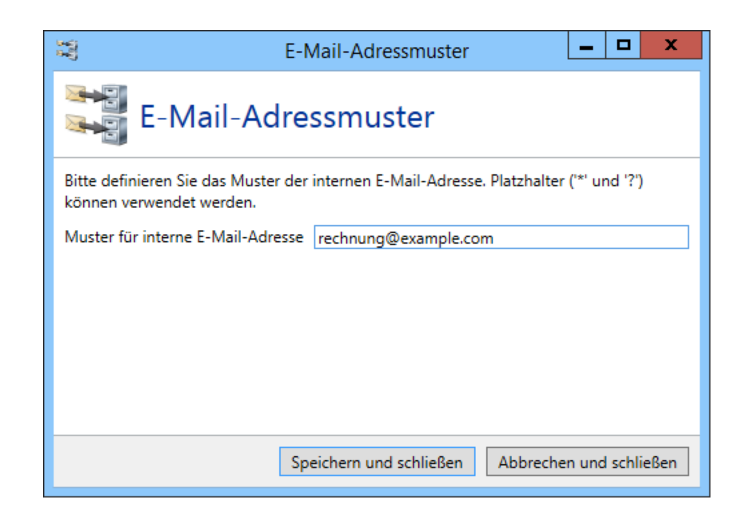


Bild 133: Neue Zuordnung erstellen

Im letzten Schritt definieren Sie in einem Profil, wie Metadaten einer E-Mail auf Metadaten im Archiv abgebildet werden. Metadaten umfassen unter anderem die Betreffzeile, Signatur- und Verschlüsselungsoptionen und andere E-Mail-Header. Um eine Verknüpfung der Werte zu erstellen, wählen Sie zunächst auf der linken Seite einen Wert aus. Wählen Sie danach aus der Liste rechts ein Feld aus dem Archiv aus. Je nach gewähltem Archivsystem kann die Liste der verfügbaren Felder sehr

lang sein. Über den Eigenschaftsfilter können Sie nach bestimmten Feldern suchen. Sobald Sie ein Feld in der Liste auswählen, wird die Zuordnung hergestellt (Bild 134).



Auf einem Profil für ein Archivpostfach werden keine Metadaten-Zuordnungen konfiguriert, da die E-Mail komplett an das Archivpostfach weitergeleitet wird und damit alle Metadaten in der E-Mail erhalten bleiben.

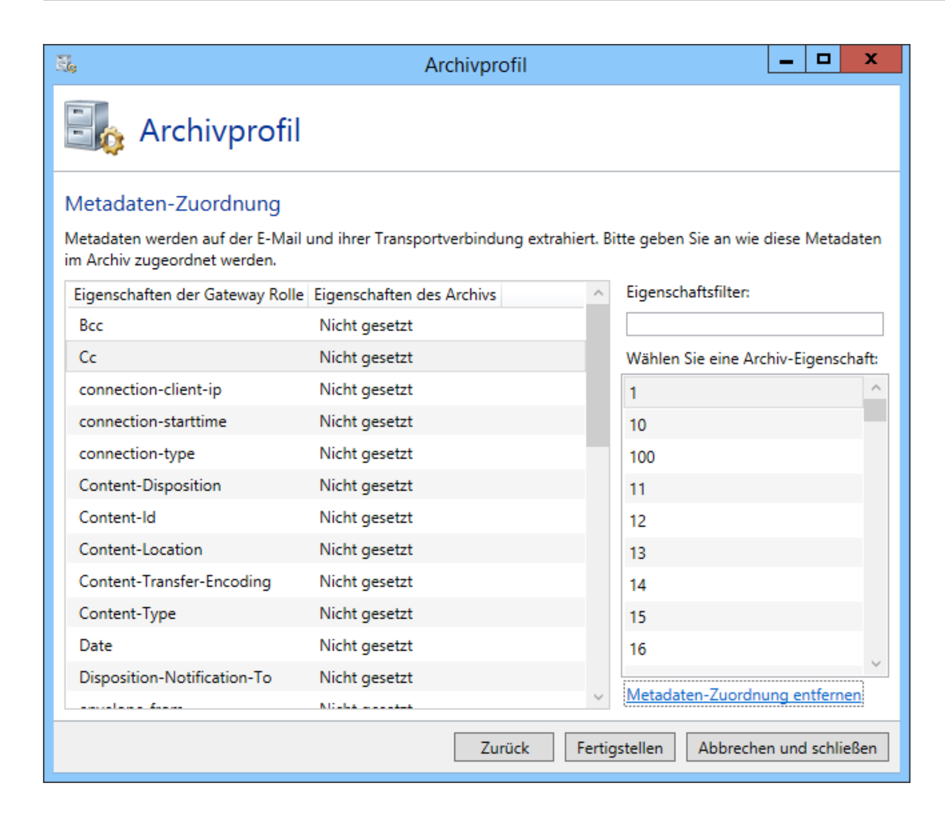


Bild 134: Metadaten-Zuordnung

Nachdem Sie mindestens ein Profil erstellt haben, ist die Konfiguration des Konnektors abgeschlossen.

Verbindung zu Mentana-Claimsoft

Für die De-Mail-Konnektoren von Mentana-Claimsoft muss eine Verbindung zu dem Web-Service dieses Anbieters eingerichtet werden (Bild 135).

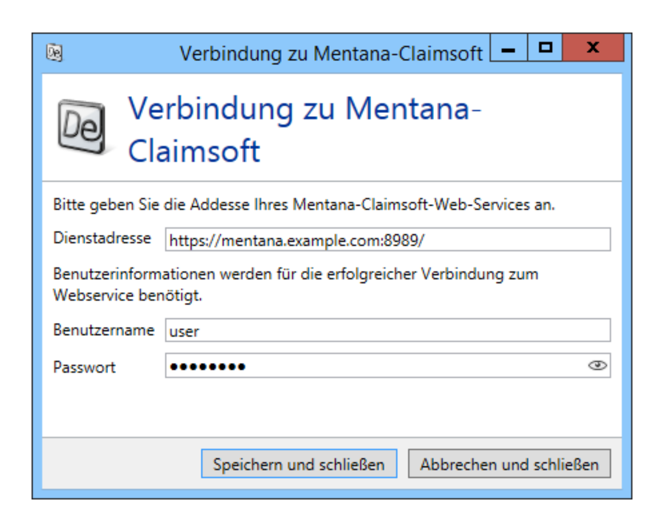


Bild 135: Verbinden Sie sich zum Mentana-Claimsoft-Webservice

Geben Sie unter **Dienstadresse** die Adresse ein, unter der der Webservice erreicht werden kann. Geben Sie unter **Benutzername** und **Passwort** die Anmeldeinformationen für den erfolgreichen Zugriff auf den Dienst ein.



Die in diesem Dialog eingegebenen Informationen sind sowohl für den De-Mail-Sendekonnektor als auch den Empfangskonnektor sofort verfügbar. Das heißt, dass Sie die Verbindung nur einmal konfigurieren müssen und Sie Ihnen sofort in allen Konnektoren bereitsteht.

Benutzer-Benachrichtigungen

Im Knoten Benutzer-Benachrichtigungen können Sie die festlegen welchen Nachrichten das Mail Gateway automatisch an interne und externe Kontakte versendet. Außerdem können Sie festlegen, welche Absenderadressen verwendet werden (Bild 136).

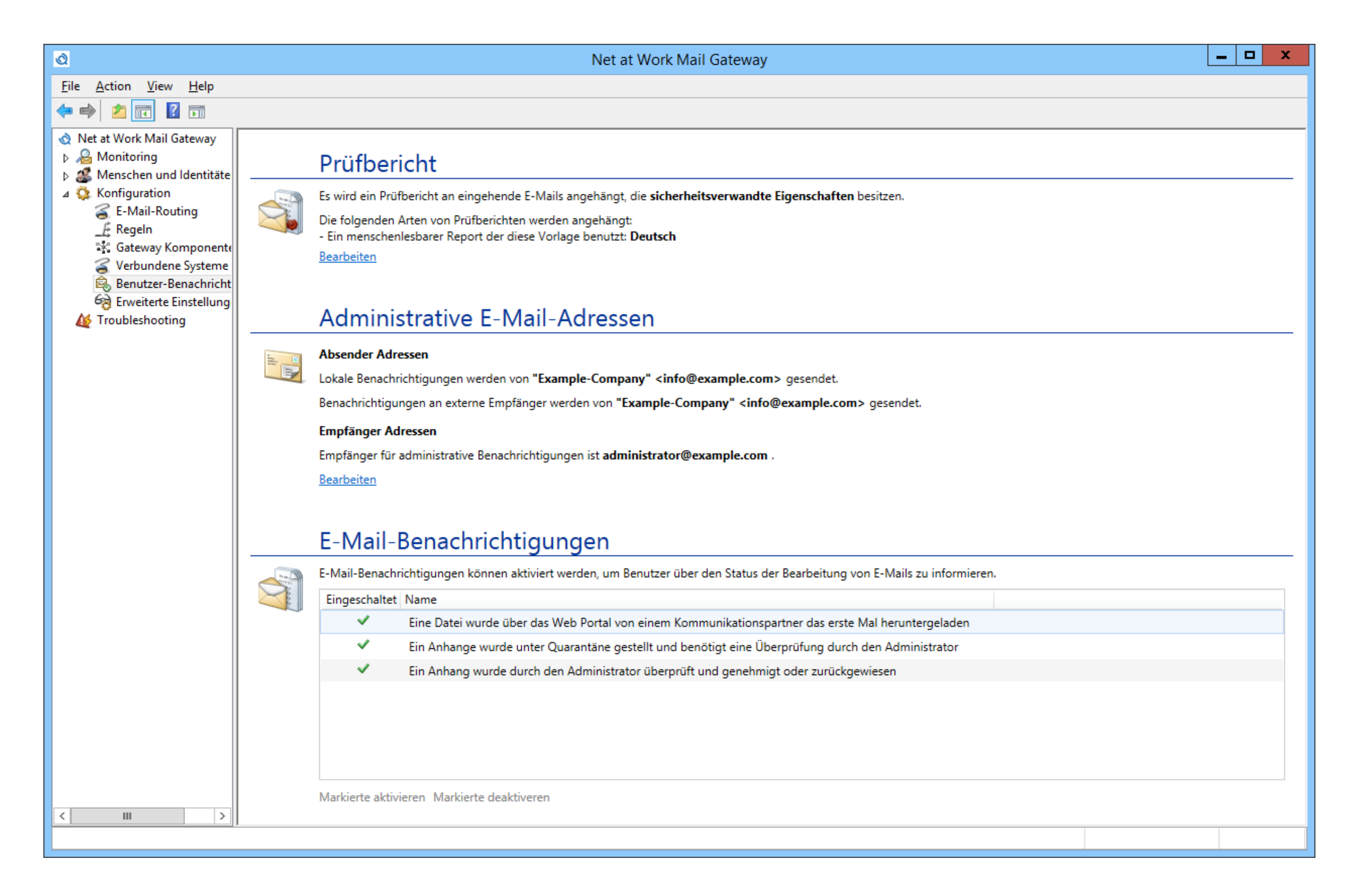


Bild 136: Benutzerbenachrichtigungen

Prüfbericht

Der Prüfbericht enthält Informationen über sicherheitsrelevante Eigenschaften und Vorgänge einer E-Mail. Er kann an eingehende E-Mails angehängt werden. Die aktuell eingestellten Werte werden in dem Knoten **Prüfbericht** angezeigt.

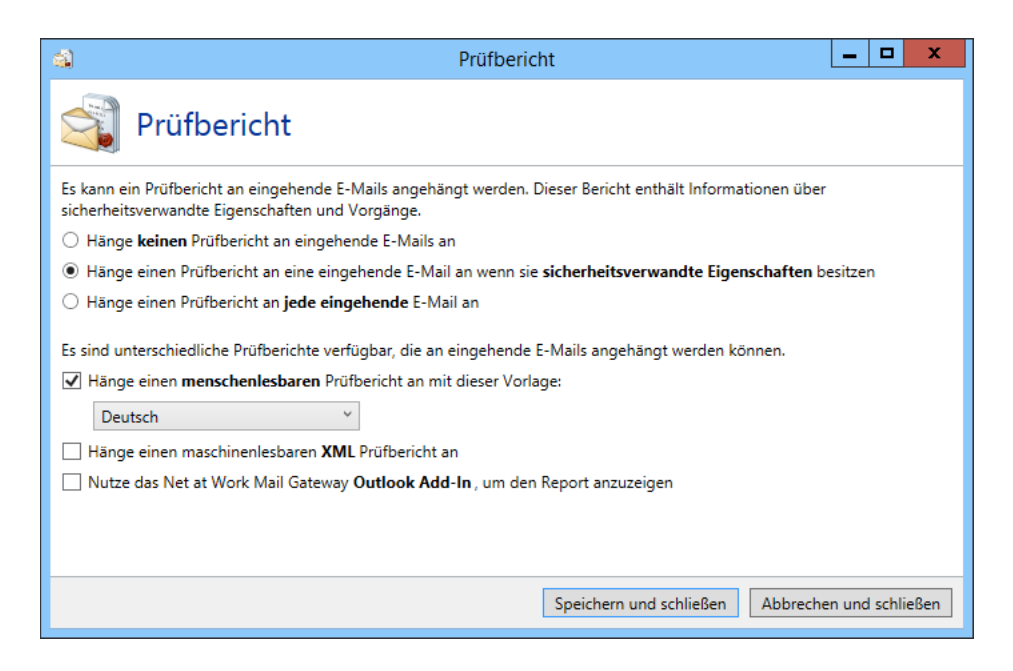


Bild 137: Der Prüfbericht

In der Konfiguration für den Prüfbericht wählen Sie zuerst aus, an welche eingehenden E-Mails der Bericht angehängt werden soll. Anschließend wählen Sie die Art des anzuhängenden Prüfberichts.

- **Menschenlesbarer Prüfbericht**
  Der Textuelle Prüfbericht stellt die Informationen in für Menschen lesbarer Form dar. Wählen Sie für den Bericht eine Vorlage, die für die Darstellung des Berichts verwendet werden soll. Standardmäßig gibt es zwei Vorlagen, eine in Deutsch und eine in Englisch. Die Vorlagen liegen in dem Konfigurationsverzeichnis der Gateway Rolle und haben die Erweiterung `HtmlProcessCardTemplate`. Falls Sie die Vorlagen anpassen wollen, dann ändern Sie bitte nicht die Standardvorlagen, da diese bei Updates der Software überschrieben werden. Legen Sie stattdessen eine Kopie einer bestehenden Vorlage an und arbeiten Sie damit.
- **XML Prüfbericht**
  Der XML Prüfbericht dient der automatischen Weiterverarbeitung der Prüfberichtsdaten durch eine weitere Anwendung.
- **Prüfbericht für das Outlook Add-In**
  Dieser Prüfbericht wird als X-Header in die E-Mail eingebettet. Diese eingebetteten Daten können vom **Outlook Add-In** des Net at Work Mail Gateways angezeigt werden.

Administrative E-Mail-Adressen

In diesem Abschnitt werden Adressen für Benachrichtigungen des Net at Work Mail Gateways hinterlegt (Bild 138). Das Net at Work Mail Gateway benötigt für die von ihm zu sendenden E-Mail-Benachrichtigungen eine gültige Absenderadresse. Abhängig davon, ob der Empfänger ein lokaler Benutzer ist oder nicht, können unterschiedliche Absenderadressen genutzt werden. Für Benachrichtigungen über bestimmte Vorfälle wird eine Empfängeradresse für diese Benachrichtigungen

benötigt. Tragen Sie die Adresse in das Feld **Empfängeradresse** ein. Die Adresse muss ebenfalls zu den eigenen Domänen gehören.

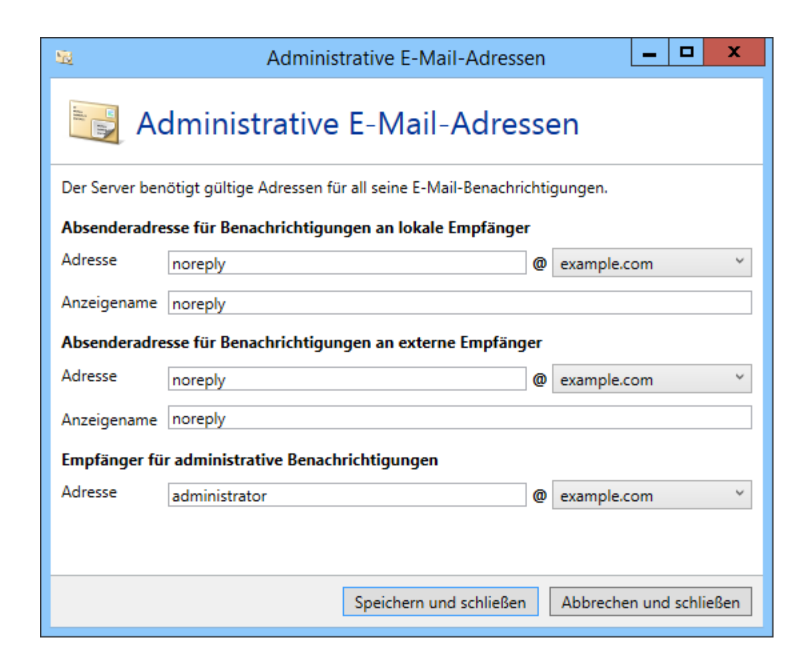


Bild 138: Die administrativen E-Mail-Adressen

Benutzer-Benachrichtigungen

Hier werden die konfigurierbaren Benachrichtigungen angezeigt. Sie können die einzelnen Benachrichtigungen markieren und aktivieren oder deaktivieren.

Erweiterte Einstellungen

Unter dem Knoten „Erweiterte Einstellungen“ finden Sie Konfigurationsmöglichkeiten, die Sie in der Regel nicht anpassen müssen. (Bild 139).

Net at Work Mail Gateway Configuration Console - [Net at Work Mail Gateway\Konfiguration\Erweiterte Einstellungen]

File Action View Help

- Net at Work Mail Gateway
  - Monitoring
  - Menschen und Identitäten
  - Konfiguration
    - E-Mail-Routing
    - Regeln
    - Allgemeine Regeleinstellungen
    - Gateway Komponenten
    - Verbundene Systeme
    - Benutzer-Benachrichtigungen
    - Erweiterte Einstellungen
  - Troubleshooting

Schutz sensibler Daten

Sensible Daten sind **geschützt.** .

Bearbeiten

Nachrichtenverfolgung

Nachrichtenübersichtsinformationen werden für **1 Monat, 0 Tage** gespeichert und ihre Details für **10 Tage, 0 Stunden** . Betreffzeilen werden **gespeichert** .

Nachrichtenstatistiken werden für **1 Jahr, 0 Monate** gespeichert.

Bearbeiten

Betreffkennzeichnungen

Fügen Sie Betreffkennzeichnungen in die Betreffzeile ein, um die Verarbeitung von ausgehenden E-Mails zu beeinflussen.

Name	Betreffkennzeichnung	Kopfzeile
PDF-Verschlüsselungspasswort	PW	X-enQsig-SymmetricEncryptionPassw
Nummer für SMS-Benachrichtigung	SMS	X-enQsig-SymmetricEncryptionNotific
Erzwinge eine Passwortbenachrichtigung des Absenders	PWBericht	X-enQsig-SymmetricEncryptionForceF
Erzwinge digitale Signatur	Signiert	X-enQsig-RequireSignature
Unterdrücke digitale Signatur	Unsigniert	X-enQsig-SuppressSignature
Erzwinge E-Mail-Verschlüsselung	Verschlüsselt	X-enQsig-RequireEncryption

Bearbeiten

Bild 139: Passen Sie erweiterte Einstellungen des Net at Work Mail Gateways an dieser Stelle an

Schutz sensibler Daten

Um sensible Daten wie z.B. kryptographische Schlüssel oder Authentifizierungsinformationen vor dem Zugriff durch Dritte zu schützen, müssen Sie diese Daten durch ein von Ihnen angegebenes Passwort verschlüsseln lassen (Bild 140). Sie können zu einem späteren Zeitpunkt das Passwort auch ändern, der Schutz der Daten kann aber nicht mehr rückgängig gemacht werden.



Sollten Sie das Passwort vergessen und die Konfiguration mit dem verschlüsselten Passwort gelöscht werden, gibt es keine weitere Möglichkeit auf die geschützten Daten zuzugreifen. Verwahren Sie deswegen immer eine Kopie des Passworts an sicherer Stelle.

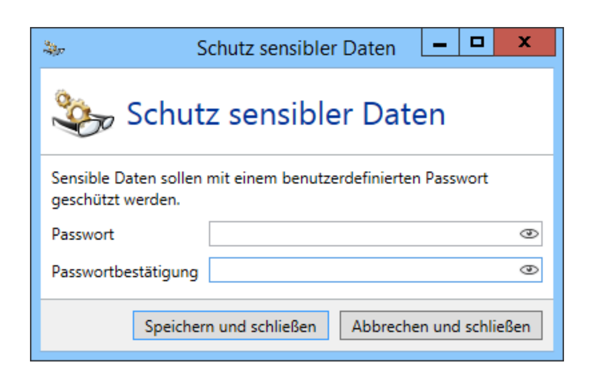


Bild 140: Das Passwort zum Schutz Ihrer Daten

Nachrichtenverfolgung

Das Net at Work Mail Gateway kann jede ein- und ausgehende Verbindung in der Nachrichtenverfolgung mitprotokollieren, damit Sie jederzeit kontrollieren können, was mit den einzelnen E-Mails geschehen ist. Diese Funktion kann über die Option **Nachrichtenverfolgung** komplett deaktiviert werden. Falls diese Option aktiviert ist, können Sie zusätzlich entscheiden, ob die Betreffzeilen der E-Mails ebenfalls gespeichert werden sollen oder ob diese von der Nachrichtenverfolgung ausgeschlossen werden sollen. Standardmäßig sind beide Optionen aktiviert.



Bitte beachten Sie die in Ihrem Unternehmen bestehenden Datenschutzvorschriften bei der Konfiguration dieses Abschnittes.

Um die Datenbankgröße der Nachrichtenverfolgung und der Reports nicht unkontrolliert wachsen zu lassen, räumt die Intranet Rolle die Datenbank in einem regelmäßigen Intervall auf. Dabei werden alle Elemente, die ein vorgegebenes Alter überschritten haben, aus der Datenbank gelöscht (Bild 141).

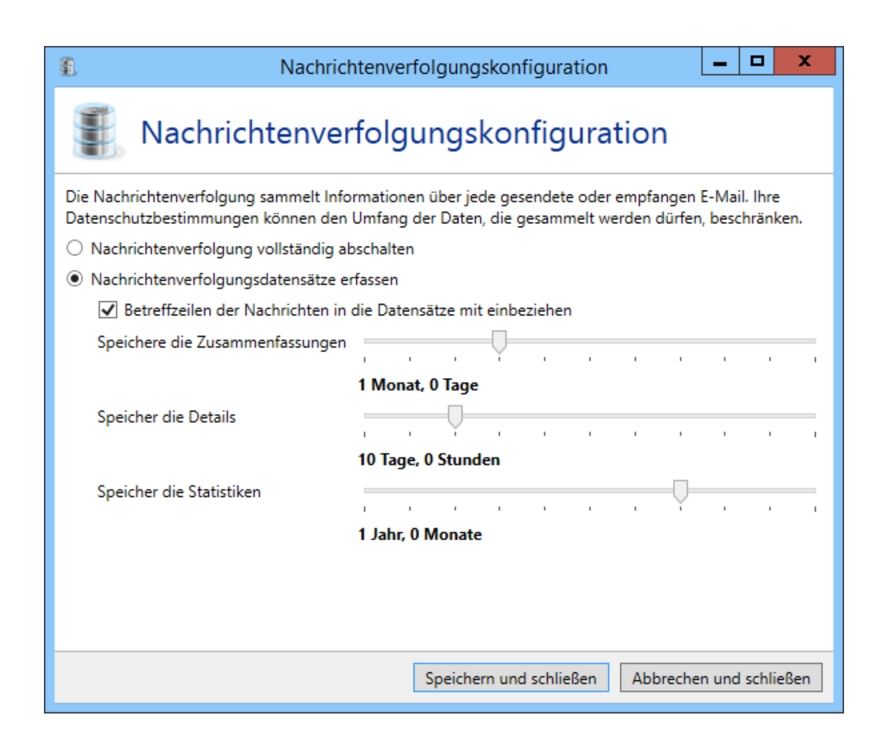


Bild 141: Anpassung der Aufbewahrungsfristen



Wenn alle Nachrichtenverfolgungsdatensätze und die statistischen Daten verworfen werden sollen, wählen Sie bitte die Option 'Nachrichtenverfolgung vollständig abschalten' unter dem Knoten 'Erweiterte Einstellungen' der Gateway Rolle. In diesem Fall werden absolut keine Daten gesammelt. Wenn Sie zum Beispiel nur die statistischen Daten aufzeichnen wollen, wählen Sie die Option **Nachrichtenverfolgungsdatensätze werden sofort gelöscht** um alle Nachrichtenverfolgungsdatensätze um 2 Uhr nachts zu löschen.

Mit dem Schieberegler **Speichere die Zusammenfassungen** stellen Sie ein, wie weit Sie generell E-Mails zurückverfolgen können wollen. Mit den Nachrichtenübersichtsinformationen können Sie lediglich in der Übersicht der Nachrichtenverfolgung sehen, ob und wann die gesuchte E-Mail angekommen ist und ob Sie angenommen oder abgewiesen wurde. Die Vorhaltezeit für die dazu gehörenden Nachrichtendetails wird mit dem Regler **Speicher die Details** eingestellt. In den Nachrichtendetails stehen die Bewertungen der einzelnen Filter, woher die E-Mail kam, wie lange die Überprüfung gedauert hat und einige nützliche Informationen mehr. Da diese Informationen den größten Teil der Nachrichtenverfolgung ausmachen, ist es möglich, diese weniger lang als die Übersichtsinformationen aufzubewahren.

Der Regler **Speicher die Statistiken** ist für den Inhalt der Reports zuständig. Mit ihm können Sie einstellen, über welchen Zeitraum Sie generell Reports erstellen können möchten.
Um einen einigermaßen aussagekräftigen Report erstellen zu können, empfehlen wir eine Mindestaufbewahrungsfrist von 12 Monaten.



Wenn Sie mehrere 10.000 E-Mails oder Spam-E-Mails pro Tag erhalten, kann das Limit der Datenbankgröße bei einem SQL Server in der Express Edition überschritten werden. Bei so vielen E-Mails sollten ggf. kürzere Aufbewahrungsfristen der Nachrichtenverfolgungsdatensätze gewählt werden oder eine SQL Server Datenbank ohne diese Beschränkung installiert werden.

Betreffkennzeichnungen

Die Betreffkennzeichnungen definieren Schlüsselwörter, um die Verarbeitung von einzelnen E-Mails zu steuern. Das Einfügen eines Schlüsselwortes in den Betreff einer E-Mail zieht dann bestimmte Aktionen nach sich. Diese Schlüsselworte werden vor dem Versand vom Net at Work Mail Gateway aus der Betreffzeile entfernt.

Nutzen Sie die Betreffkennzeichnungen, in dem Sie am Anfang oder Ende der Betreffzeile in Klammern die Schlüsselworte aus der folgenden Liste angeben, die Ihre Aufgaben definieren. Leerzeichen und Unterschiede zwischen Groß- und Kleinschreibung werden im Schlüsselwort ignoriert. Das bedeutet, dass die folgenden Beispiele das gleiche Resultat ergeben. Alternativ können Sie auch das **Net at Work Mail Gateway Outlook Add-In** nutzen.

Standardmäßig werden eckige Klammern verwendet, um die Betreffkennzeichnungen kenntlich zu machen. Über den Dialog zum Bearbeiten der Markierung können sie festlegen, welche Art von Markierung verwendet werden soll (Bild 142).

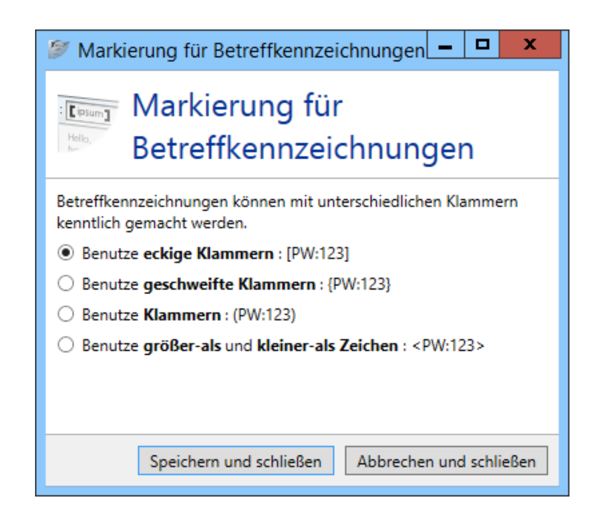


Bild 142: Konfigurieren Sie die Marker für Betreffkennzeichnungen

Beispiele für den Einsatz von Betreffkennzeichnungen in der Betreffzeile:

```
[pw:geheim4312] Hiermit sende ich Ihnen das verschlüsselte Dokument

[ PW : geheim4312 ] Hiermit sende ich Ihnen das verschlüsselte Dokument
```

Oder auch mehrere Kennzeichnungen gleichzeitig in einer Klammer `[Unverschlüsselt, PDF, PW:geheim4312] Hiermit sende ich Ihnen das verschlüsselte Dokument`

Oder auch mehrere Kennzeichnungen gleichzeitig in unterschiedlichen Klammern `[Unverschlüsselt] [PDF] [PW:geheim4312] Hiermit sende ich Ihnen das verschlüsselte Dokument`



Die Betreffkennzeichnungen müssen am Anfang oder am Ende der Betreffzeile stehen, um Ordnungsgemäß verarbeitet zu werden.



In Abhängigkeit der von Ihnen lizenzierten Funktionen können Ihnen andere Kennzeichnungen zur Verfügung stehen als die im obigen Beispiel genannten. Die obigen Hinweise gelten bei allen Kennzeichnungen.

Die folgenden Betreffkennzeichnungen stehen Ihnen zur Verfügung:

- **[Versandbestätigung]**
  De-Mail: Fordert eine Versandbestätigung von De-Mail an. Entspricht einen Einschreiben bei Briefen.
- **[Eingangsbestätigung]**
  De-Mail: Fordert eine Empfangsbestätigung von De-Mail an. Entspricht einem Einwurf-Einschreiben bei Briefen.
- **[Abholbestätigung]**
  De-Mail: Fordert eine Abholbestätigung von De-Mail an.
- **[Absenderbestätigt]**
  De-Mail: Setzt den Status 'Absenderbestätigt' in De-Mails.
- **[Persönlich]**
  De-Mail: Setzt den Status 'Privat' in De-Mail. Entspricht einem Einschreiben Eigenhändig bei Briefen.
- **[LFT]**
  Diese Kennzeichnung wird nur vom Outlook Add-In für den **Large File Transfer** verwendet.

Sie können die Betreffkennzeichnungen an Ihre Bedürfnisse anpassen (Bild 143) und auch wieder auf ihre Standardwerte zurücksetzen.



Im Outlook Add-In können Sie einstellen, dass an Stelle der X-Header die Betreffkennzeichnungen verwendet werden. Nehmen Sie in diesem Fall keine Änderungen in diesem Bereich vor. Das Add-In wird sonst nicht mehr funktionieren.

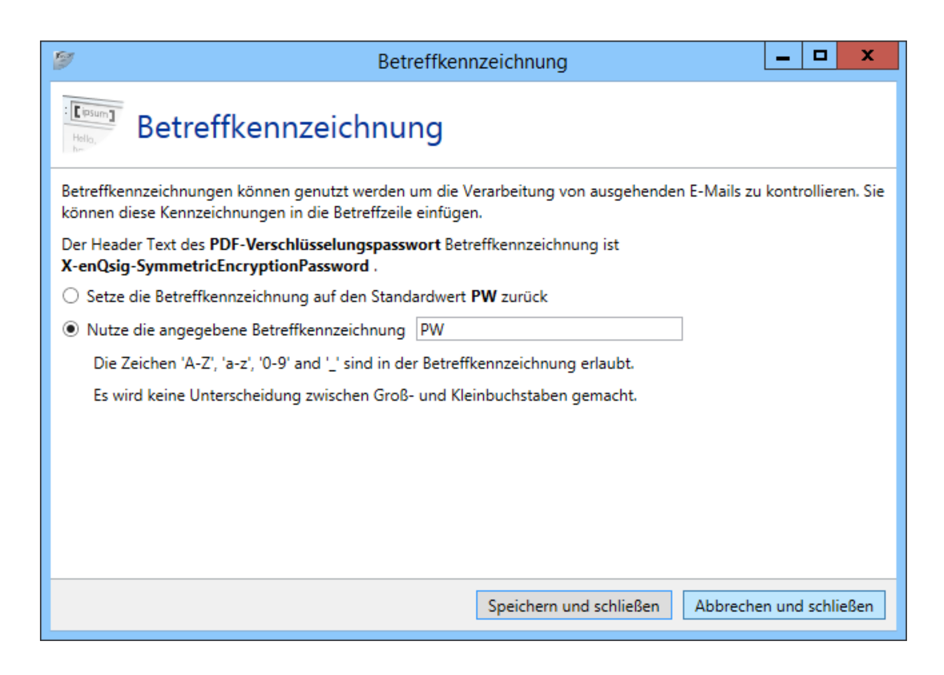


Bild 143: Betreffkennzeichnungen bearbeiten

Beim automatisierten Versand von E-Mails können Sie anstatt der Betreffkennzeichnungen auch E-Mail-Header in die Nachricht einfügen, um diese Informationen anzugeben. Die E-Mail-Header werden im Folgenden erklärt. In der Oberfläche finden Sie neben der Betreffkennzeichnung den dazu gehörigen X-Header.



Anstatt der Nutzung der 'Betreffkennzeichnungen' können Sie auch das **Outlook Add-In** für das Net at Work Mail Gateway installieren. Das Outlook Add-In wird an Stelle der Betreffkennzeichnungen mit Outlook 2007 und Outlook 2010 verwendet.

Level-of-Trust-Konfiguration

Das Level-of-Trust-System ist ein mehrschichtiges Konzept, das die Vertrauenswürdigkeit einer Kommunikationsbeziehung oder einer Domäne beurteilt. „Vertrauen“ muss sich ein Absender verdienen. Stärkster Pluspunkt dabei ist eine verlässliche und dauerhafte Verbindungshistorie.

Das System bewertet verschiedene Kriterien, u.a. Absenderadressen und Prüfsummen, vor allem aber auch die Adressbeziehungen für eingehende und ausgehende E-Mails.

Bei ausgehenden E-Mails wird die Kommunikationsbeziehung (zwischen Absender und Adressat) in der Datenbank mit einem sehr hohen Vertrauensbonus gespeichert. Um diese Daten zu schützen, wird die Beziehung nicht im Klartext gespeichert, sondern nur in Form eines Hashwertes (Prüfsumme) festgehalten. Des Weiteren ist die Relation von Absender, Betreff und Domäne des Empfängers eine interessante Perspektive. Es liegt nahe, auch eine Antwort eines Kollegen oder eines Stellvertreters, und gegebenenfalls eine alternative Adresse, als „gut“ bewerten zu können. Zusätzlich wird bei ausgehenden E-Mails das Vertrauen in die Domäne des Adressaten um einen bestimmten Wert erhöht. Damit erhalten

auch die Antwort-E-Mails des Adressaten an andere Nutzer des Systems einen Bonus. Wird eine eingehende E-Mail als Spam klassifiziert, verringert sich das Vertrauen in die Domäne.

Findet über einen gewissen Zeitraum keine Kommunikation mit einem bestimmten Absender mehr statt, verringert sich der Level of Trust automatisch. Diese Abnahme des Wertes geschieht sowohl bei Bonus- als auch bei Malus-Werten. Einem längeren „Schweigen“ wird auf diese Art und Weise sowohl im Positiven wie auch im Negativen Rechnung getragen: verlässliche, dauerhafte Kommunikation hinterlässt einen immer besseren Eindruck, Spam-Wiederholungstäter einen immer schlechteren.

Das Level-of-Trust-System muss pro Regel aktiviert werden. Die Einstellungen werden jedoch im Menü „Level of Trust“ global vorgenommen (Bild 144).

Allgemeine Einstellungen

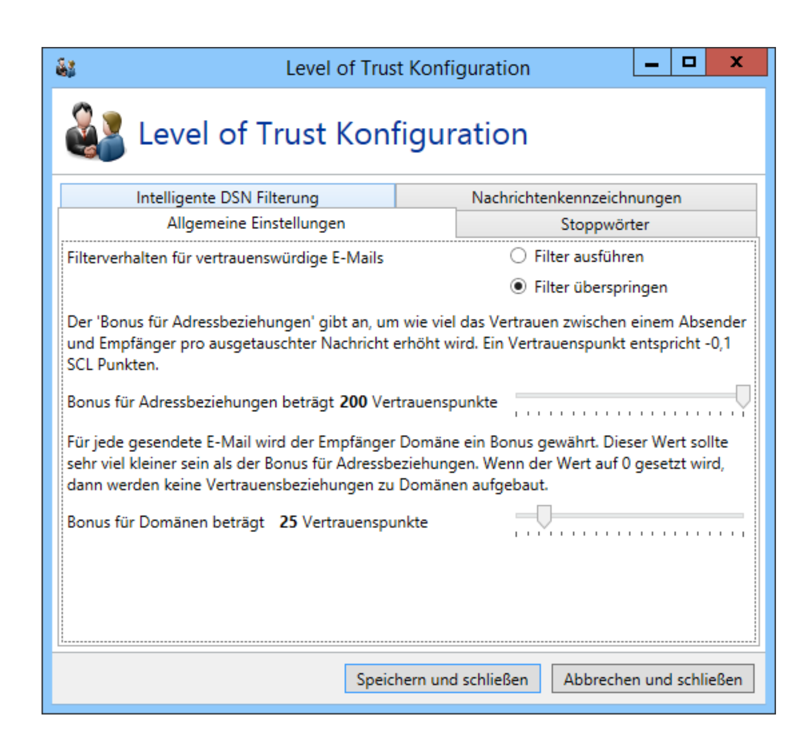


Bild 144: Definieren Sie die allgemeinen Einstellungen des Level-of-Trust-Systems

Wenn die Funktion **Filter für vertrauenswürdige E-Mails überspringen** aktiviert wird, werden eingehende E-Mails mit einer hinreichend hohen Level-of-Trust-Bewertung als vertrauenswürdig markiert. Filter, die auf einer Regel definiert sind, werden dann übersprungen. Lediglich Aktionen, wie zum Beispiel die Anhänge verwalten Aktion oder die CYREN-Premium-Antivirus-Aktion können die Annahme der E-Mail dann noch verhindern.

Mit der Einstellung **Bonus für Adressbeziehungen** legen Sie fest, um wie viele Punkte das Vertrauen zwischen einem Absender und einem Empfänger pro ausgehender Nachricht erhöht wird (Adressbeziehung). Mit dem Schieberegler können Sie hier einen Wert zwischen 0 und 200 einstellen. Ein Punkt entspricht dabei (-0,1) Punkten für den SCL.

Für jede ausgehende E-Mail wird nicht nur der sogenannte Adressbeziehungsbonus erhöht, sondern auch ein Bonus für die jeweilige Empfängerdomäne. Um wie viele Punkte das geschieht, stellen Sie mit dem Schieberegler **Bonus für Domänen beträgt...** ein. Dieser Wert sollte kleiner sein als der Bonus für Adressbeziehungen. Auch hier können Sie mit dem Schieberegler einen Wert zwischen 0 und 200 einstellen. Ein Punkt entspricht auch dabei (-0,1) Punkten für den SCL.

Stoppwörter

Auf der Registerkarte **Stoppwörter** definieren Sie die sogenannten Stoppwörter (Bild 145).

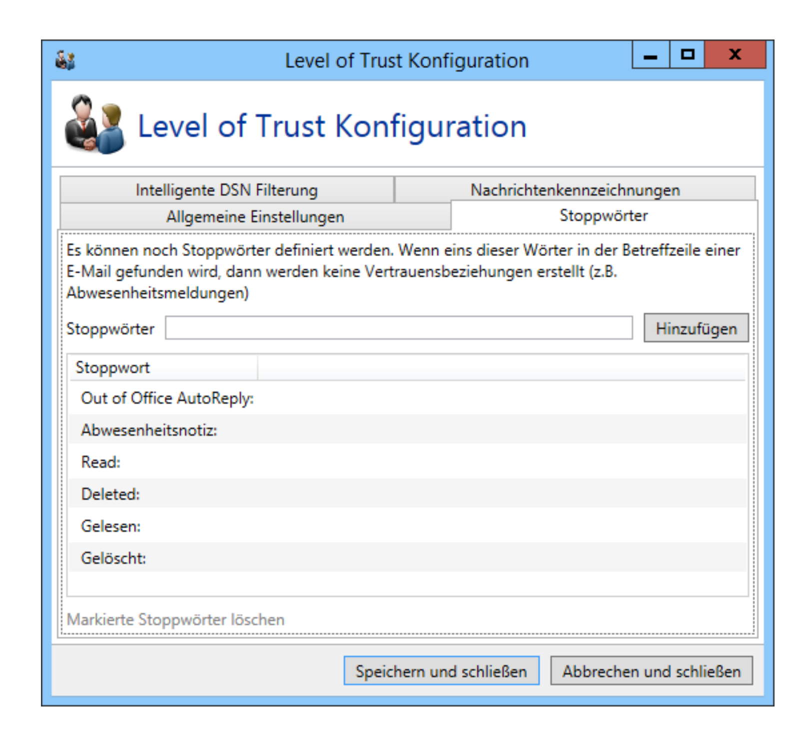


Bild 145: Definieren Stoppwörter, die Veränderungen der Level-of-Trust-Beziehungen unterbinden

Sobald die Gateway Rolle eines dieser Wörter im Betreff einer ausgehenden E-Mail findet, bleiben der Adressbeziehungsbonus als auch der Domänen Bonus gleich und werden nicht erhöht. Bei automatisch generierten E-Mails wie Abwesenheitsnotizen ist das eine sinnvolle Einstellung.

Intelligente DSN-Filterung

Die intelligente DSN-Filterung überprüft eingehende Delivery Status Notifications (DSNs). Da das Mail Gateway weiß, welche E-Mails aus dem Unternehmen versendet wurden, kann die Software auch feststellen, ob für den gerade vorliegenden DSN eine entsprechende E-Mail das Unternehmen verlassen hat (Bild 146).

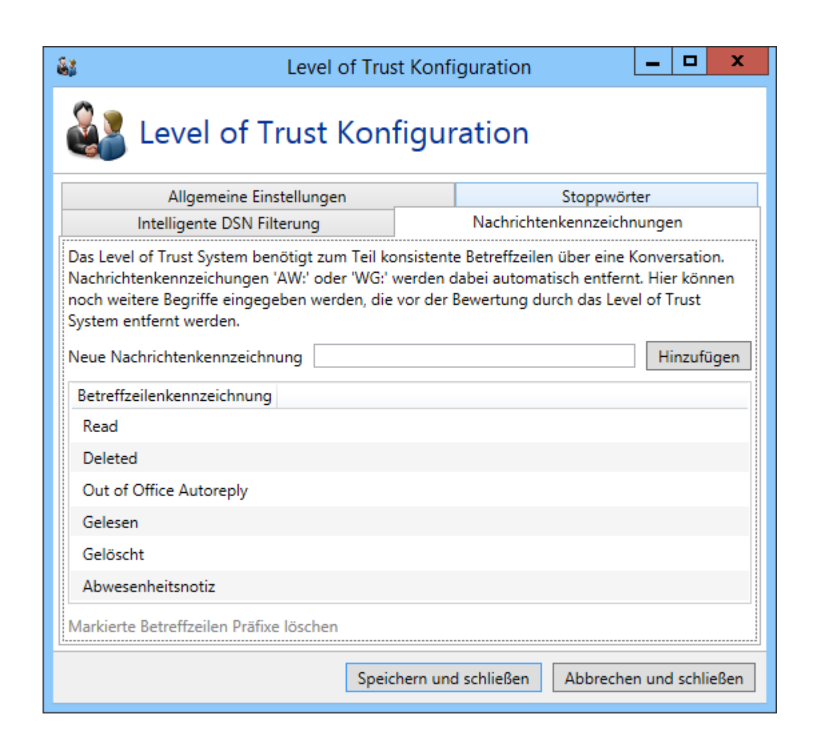


Bild 146: Konfigurieren Sie die Intelligente DSN-Filterung

Ein Beispiel: Es kommt ein DSN an und das Mail Gateway stellt fest, dass die Originalnachricht für diesen DSN von schmidt@example.com an schulze@netatwork.de gesendet wurde. Dann überprüft das Mail Gateway, ob es ein Adresspaar schmidt@example.com/schulze@netatwork.de in der Level-of-Trust-Datenbank gibt. Wenn das nicht der Fall ist, kann der vorliegende DSN nicht gültig sein und erhält Maluspunkte. Findet sich ein passendes Adresspaar, erhält der DSN Bonuspunkte.

Damit diese Überprüfung stattfinden kann, müssen zwei Voraussetzungen gegeben sein: Zum einen muss ein RFC-konformer DSN vorliegen. Das bedeutet, dass die Originalnachricht als Anhang an dem DSN hängt, damit das Mail Gateway das Original-Adresspaar ermitteln kann. Des Weiteren muss sichergestellt sein, dass das Mail Gateway alle ausgehenden E-Mails des Unternehmens wirklich kennt. In Netzwerken mit verteilten Internetanbindungen kann das unter Umständen ein Problem sein.

Mit der Einstellung **Intelligente DSN-Filterung** können Sie die intelligente DSN-Filterung direkt beeinflussen. Setzen Sie den Radio-Button auf **Automatisch**, wird das Mail Gateway zunächst in der Level-of-Trust-Datenbank nachsehen, ob sich darin Elemente befinden, die älter als 7 Tage sind. Erst wenn das gegeben ist, wird das Mail Gateway ankommende DSNs bewerten. Das ist auch die Standardeinstellung. Wenn Sie den Radio-Button auf **Aktiviert** setzen, wird das Mail Gateway den DSN immer bewerten, auch wenn noch keine Datensätze in der Level-of-Trust-Datenbank stehen. Um die intelligente DSN-Filterung abzuschalten, setzen Sie den Radiobutton auf **Deaktiviert**.

Nachrichtenkennzeichnungen

Das Level-of-Trust-System benötigt zum Teil konsistente Betreffzeilen über eine Konversation. Nachrichtenbezeichnungen wie z.B. ‚AW:‘ oder ‚WG:‘ müssen dazu entfernt werden. Auf der

Registerkarte **Nachrichtenkennzeichnungen** konfigurieren Sie alle Kennzeichnungen, die Ihr E-Mail-System verwendet (Bild 147).

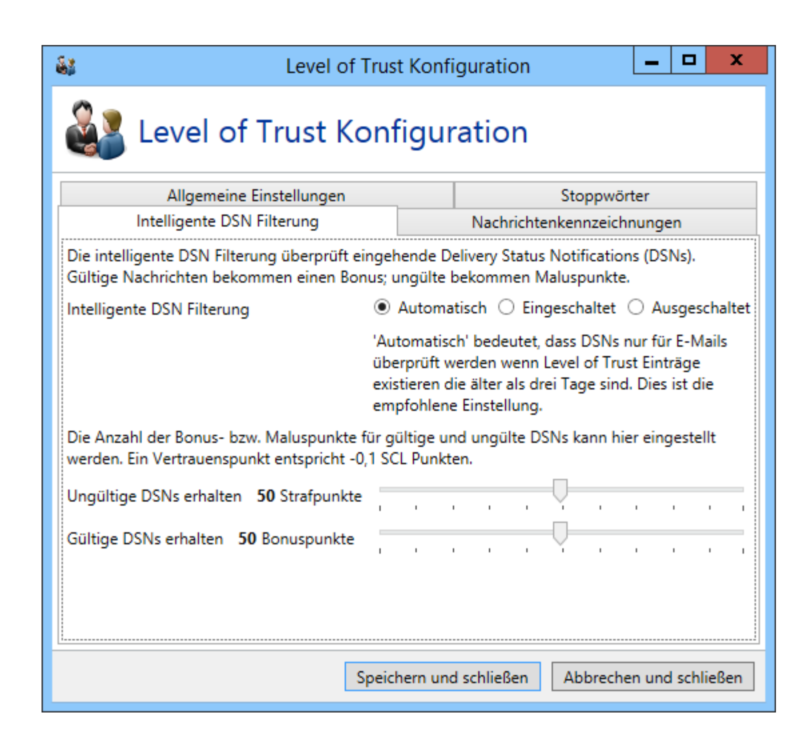


Bild 147: Definieren Sie Nachrichtenkennzeichnungen, die in den Betreffzeilen Ihrer E-Mails vorkommen

SMTP-Protokolleinstellungen

Die Protokolleinstellungen regeln das Verhalten beim Empfang von E-Mails, die SMTP-Timeouts und die SMTP-Statusmeldungen.

Verhalten

Wenn eine E-Mail an mehrere Empfänger geht, kann es sein, dass abhängig von den Empfängern unterschiedliche Regeln für diese E-Mail greifen. Das Net at Work Mail Gateway kann, bei entsprechender Einstellung, das einliefernde System dazu zwingen, für jeden einzelnen Empfänger eine eigene E-Mail zu schicken.

Diese Einstellung beugt Konflikten bei mehrfach adressierten E-Mails vor, wenn eine E-Mail über eine Verbindung an zwei Empfänger versendet wird und dabei zwei verschiedene Regeln zutreffen würden. Durch die Verwendung von SMTP ist es nicht möglich, für einzelne Empfänger unabhängige Rückmeldungen zu liefern. Es kann immer nur die komplette Verbindung beendet werden.

Durch die Konfiguration der Option **Anwendung von Regeln** können Sie das Net at Work Mail Gateway anweisen, an das einliefernde System die Fehlermeldung „Too many Recipients“ zu senden, sofern Empfänger mit kollidierenden Regeln gesendet werden (Bild 148).

Laut RFC ist dies allerdings erst ab dem 101. Empfänger erlaubt, auch wenn bislang keine E-Mail-Server bekannt sind, die durch dieses Verhalten gestört werden.

Durch diese Einstellung wird jede E-Mail mit genau einem Empfänger versendet. So kann das Net at Work Mail Gateway für jeden Empfänger die passende Regel anwenden. Allerdings werden die E-Mails entsprechend mehrfach vom Absender eingeliefert.

Die Aktivierung dieser Funktion erlaubt Ihnen die Steuerung der E-Mail-Bewertung für den Preis einer mehrfachen Übertragung und einem nicht ganz RFC-konformen Verhalten.

Ist diese Option deaktiviert, dann wird die Regel, die für den ersten Empfänger zutrifft, auf alle Empfänger dieser E-Mail angewendet.

Für alle anderen Empfänger gilt das gleiche Resultat.

Das Net at Work Mail Gateway kann erkennen, wenn dieselbe E-Mail mehrere Male empfangen wird. Das mehrfache Versenden derselben E-Mail tritt üblicherweise bei falscher Konfiguration, wie z.B. E-Mail-Schleifen, auf. Sie können einstellen, ob die E-Mails verworfen werden sollen, oder nicht, und wie groß das Zeitfenster für die Erkennung ist.

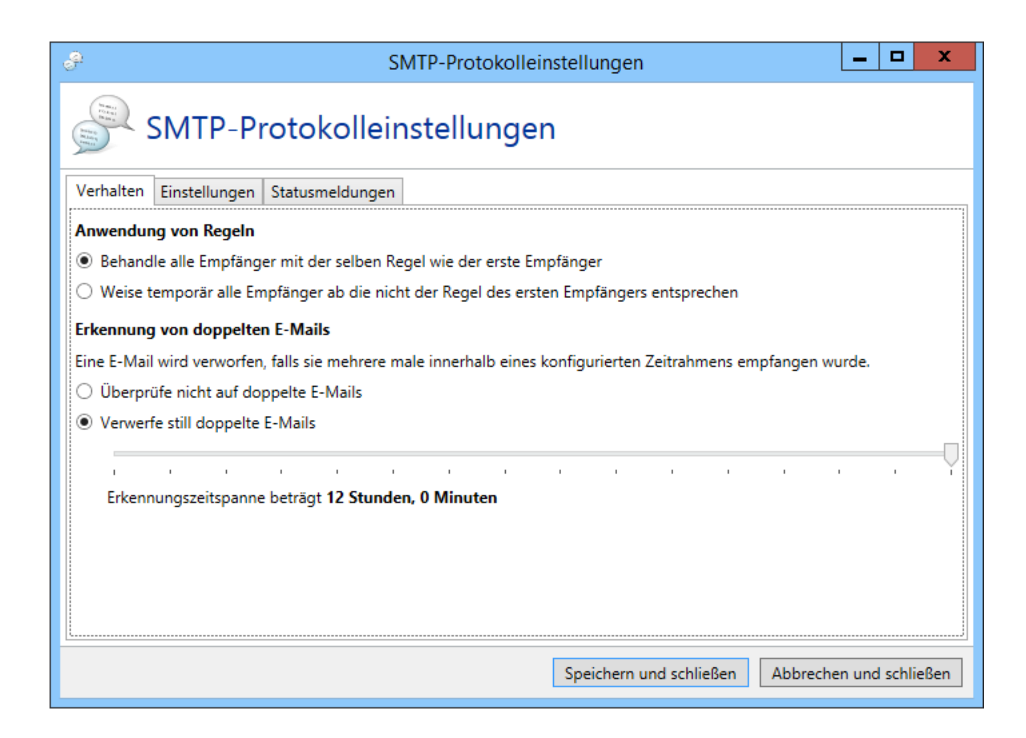


Bild 148: Verhalten beim Empfang von Nachrichten

Einstellungen

Das Anpassen der Timeouts und der Größenbeschränkung (Bild 149) hat großen Einfluss auf den Ressourcenbedarf Ihres Servers bei starkem E-Mail-Verkehr.

Im Abschnitt **SMTP Protokoll Timeout Einstellungen** können Sie festlegen, ab wann das Net at Work Mail Gateway bei Inaktivität eine Verbindung trennt. Dies wird für zwei Abschnitte innerhalb des SMTP-Protokolls festgelegt.

Mit der Einstellung **Envelope-Timeout beträgt n Sekunden** stellen Sie den Timeout für die Kommandos innerhalb des sogenannten Envelope Teils ein. Das betrifft alle Kommandos bis zum DATA-Befehl (HELO/EHLO, MAIL FROM, RCPT TO). Sobald der DATA-Befehl gesendet wurde, gilt die Einstellung **Body-Timeout beträgt n Sekunden**. Eine Trennung der Timeouts ist sinnvoll, da bei der Übertragung des Body Teils, durch dazwischen geschaltete Filter und Aktionen, eher Timeouts auftreten können als beim Envelope. Dieser wird bei einer normalen Übertragung sehr zeitnah und flüssig übertragen. Eine längere Wartezeit in diesem Teil der Mailübertragung deutet eher auf einen DoS-Angriff oder ähnliches hin. Daher haben Sie die Möglichkeit im Notfall den Timeout des Envelope Teils zu reduzieren. Mit den Schiebereglern bei den jeweiligen Einstellmöglichkeiten können Sie einen Wert zwischen 30 und 600 Sekunden einstellen.

Über die Einstellung **Größenlimit** können Sie einstellen, ob das Mail Gateway E-Mails mit beliebiger Größe annimmt oder nicht.

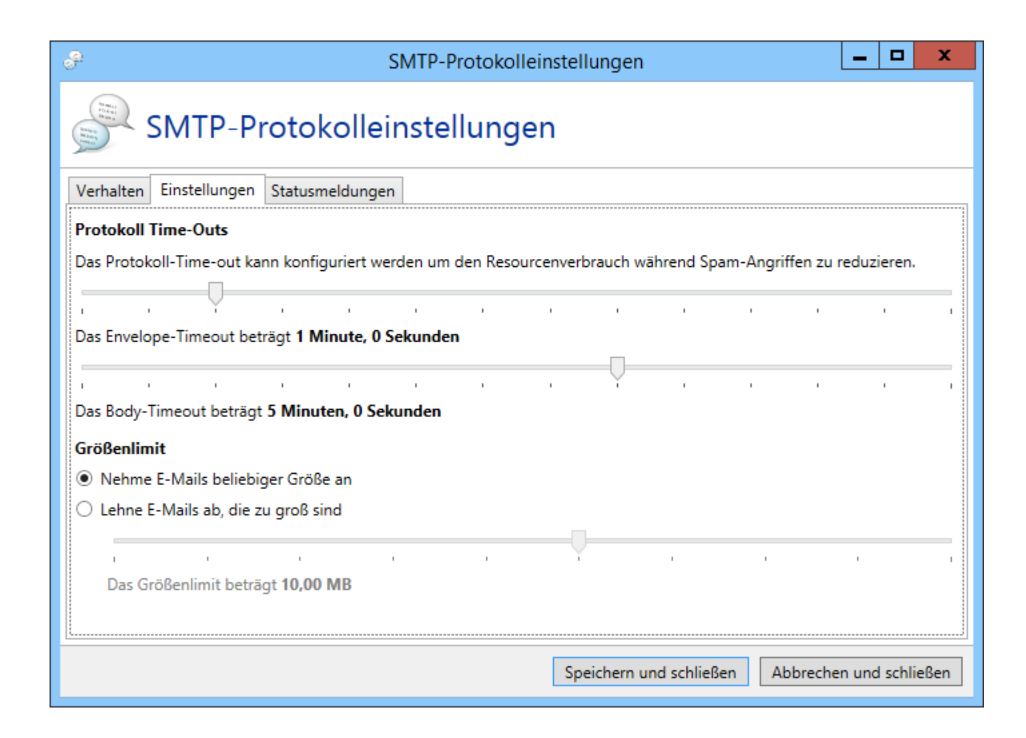


Bild 149: Timeouts und Größenlimits

Statusmeldungen

Die Statusmeldungen (Bild 150) bestimmen mit welchen Texten sich das Gateway gegenüber anderen Servern meldet.

Die SMTP Antworten sind Standardangaben im SMTP-Handshake, die für den normalen User in der Regel nicht sichtbar sind. Dennoch kann es sinnvoll sein, die Angaben nach eigenem Bedarf zu ändern.

Auf diese Art und Weise können Administratoren bei einer Fehlersuche die E-Mails mitunter leichter analysieren. Die Meldungen „Rejected mail“ und „Blacklisted Address“ sind beispielsweise wichtige Informationen für den Absender einer geblockten E-Mail.

Um eine Meldung zu ändern, klicken Sie einfach in das zugehörige Eingabefeld und ändern den Text.



Für SMTP Meldungen dürfen Sie keine Umlaute verwenden. Umlaute werden von dem verwendeten SMTP Protokoll nicht unterstützt.

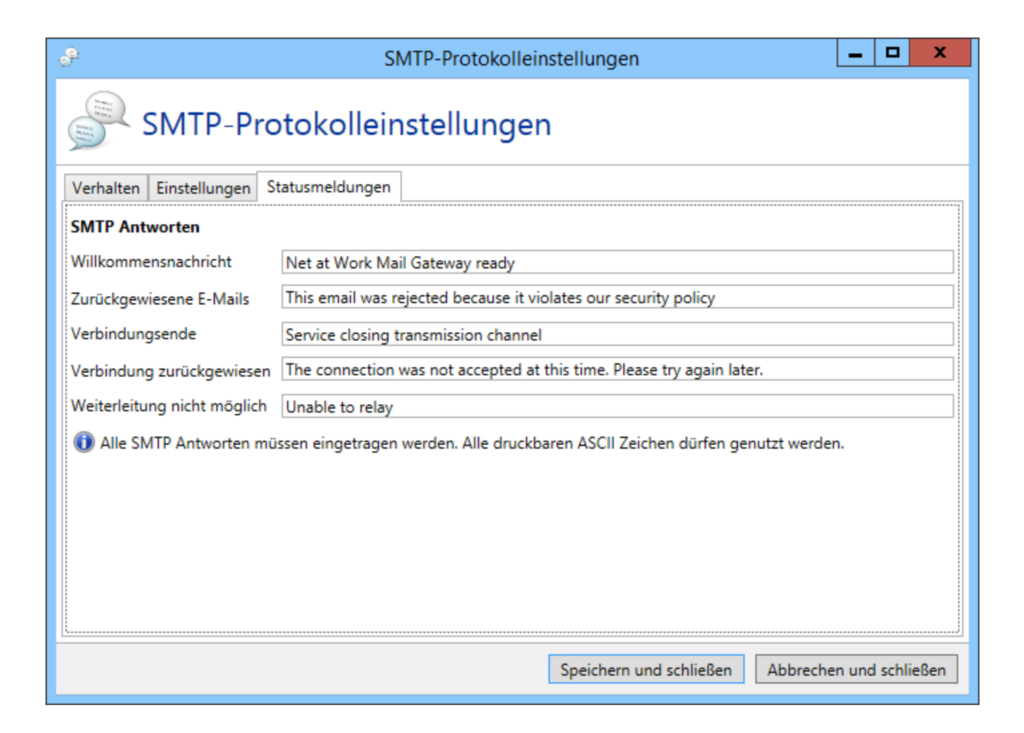


Bild 150: Textuelle SMTP-Statusmeldungen des Gateways an andere Server

SSL/TLS-Konfiguration

Bei der Transportverchlüsselung wird die Verbindung über SSL oder TLS abgesichert. Dabei greift die Gateway Rolle auf das Betriebsystem zurück und dessen Einstellungen werden bei Verbindungen verwendet. Im letzter Zeit haben sich einige Verschlüsselungsverfahren (z.B. DES oder RC-4) als nicht mehr sicher herausgestellt. Daher ist sinnvoll, diese zu deaktiveren. Einige Cipher Suites unterstützen ein Verfahren namens Perfect Forward Secrecy. Dies verhindert, kurz gesagt, das die Inhalte von Verbindungen von unbefugten dritten entschlüsselt werden können, selbst wenn der private Schlüssel des Server-Zertifikats bekannt ist. In der Standardeinstellung verwendet Windows diese Verfahren aber nicht bevorzugt. Sie können daher hier in der Oberfläche die empfohlenen Einstellungen anwenden (Bild 151). Damit die Änderungen wirksam werden, muss der Server neu gestartet werden. Dies können Sie direkt in dem Dialog veranlassen.



Hierbei handelt es sich um eine Systemweite Änderung, die sich auch auf andere Programme auswirken kann.

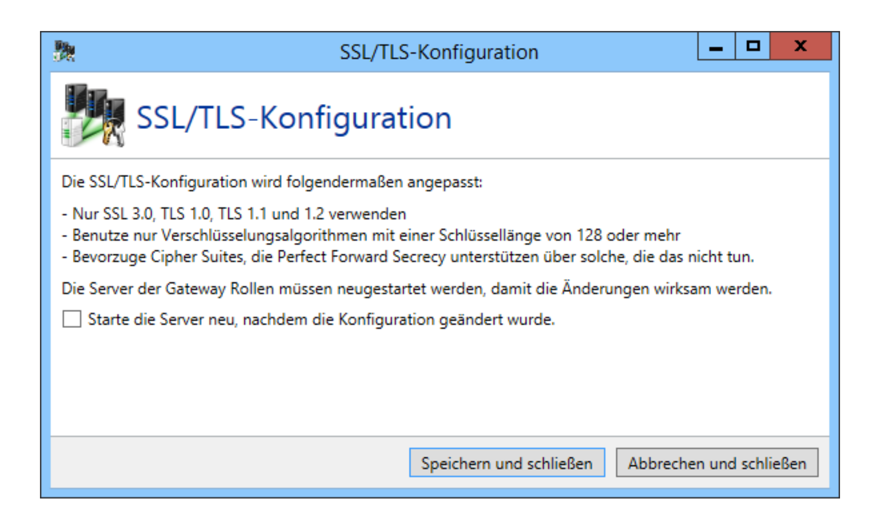


Bild 151: Empfohlene Einstellungen für die SSL/TLS-Konfiguration von Windows anwenden

Sie haben in diesem Bereich außerdem die Möglichkeit, die Standardwerte von Windows wiederherzustellen (Bild 152). Auch hier ist wieder ein Neustart des Servers notwendig, den Sie über den Dialog veranlassen können.

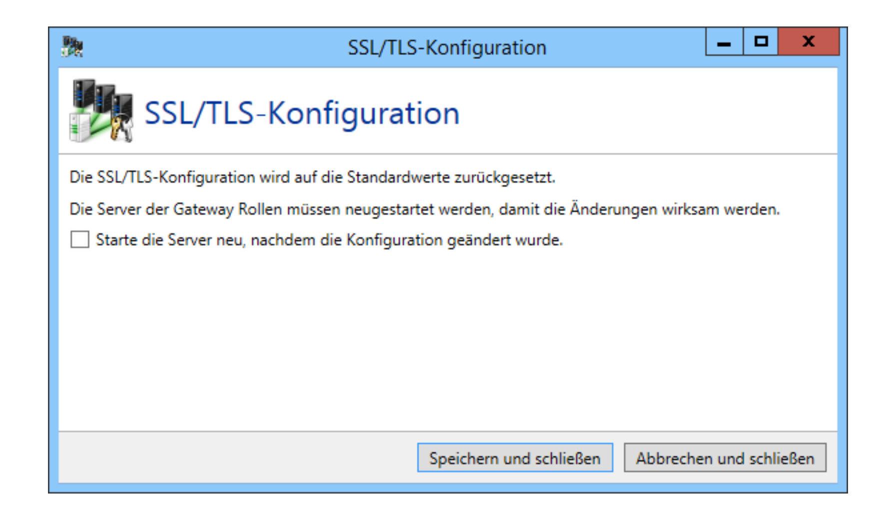


Bild 152: Auf Standardwerte für die SSL/TLS-Konfiguration zurückfallen

9. Troubleshooting

Unter dem Menüpunkt **Troubleshooting** befinden sich Werkzeuge, um Protokolle der Aktivitäten oder auch eine neue Datenbank für die einzelnen Rollen des Mail Gateways zu erstellen (Bild 153). Das erneute Erstellen einer Datenbank kann notwendig werden, falls die alte Datenbank Schaden genommen hat.

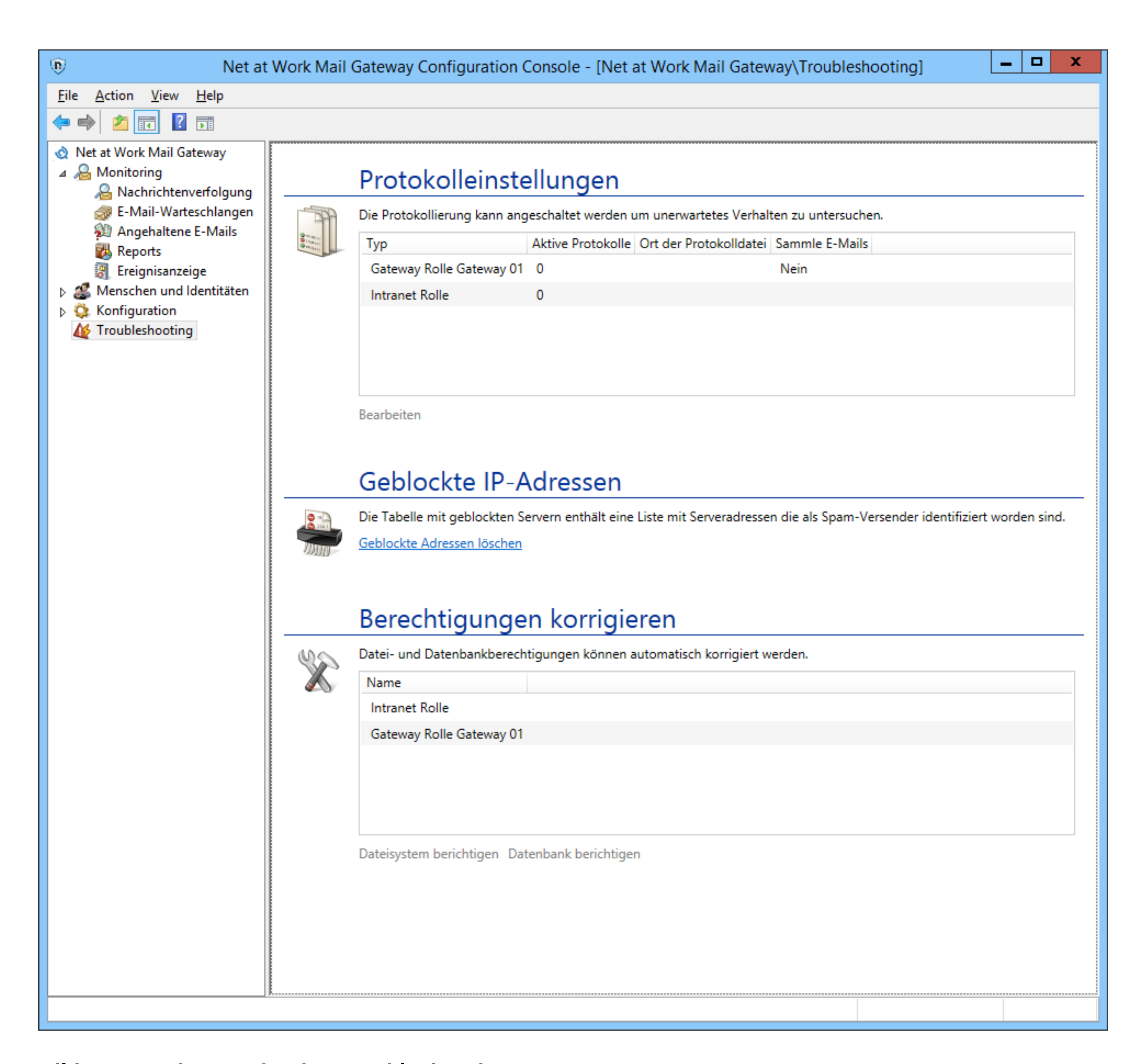


Bild 153: Werkzeuge für das Troubleshooting

Protokoll Einstellungen

Konfigurieren Sie in der ersten Karteikarte den Speicherort für die Log-Dateien und wählen Sie die Kategorien, für die Sie die Protokollierung aktivieren möchten (Bild 154).



Je nachdem, welche Kategorien Sie hier auswählen, können die Logdateien sehr schnell mehrere hundert Megabytes groß werden. Wählen Sie für die Dateien ein Laufwerk, auf dem genug Speicherplatz frei ist.

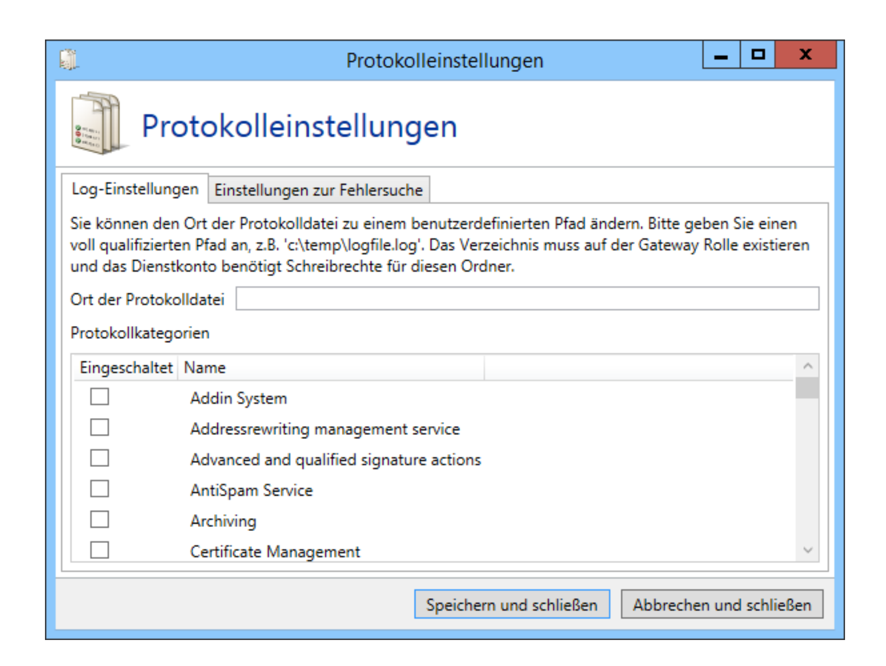


Bild 154: Konfigurieren Sie die Protokoll-Einstellungen

In der Karteikarte **Einstellungen zur Fehlersuche** können Sie zusätzlich alle ein- und ausgehenden E-Mails vor und nach der Bearbeitung durch das Net at Work Mail Gateway auf die Festplatte schreiben lassen (Bild 155). Dieser Reiter ist nur bei Gateway Rollen vorhanden. Auf der Intranet Rolle können Sie dies nicht konfigurieren.

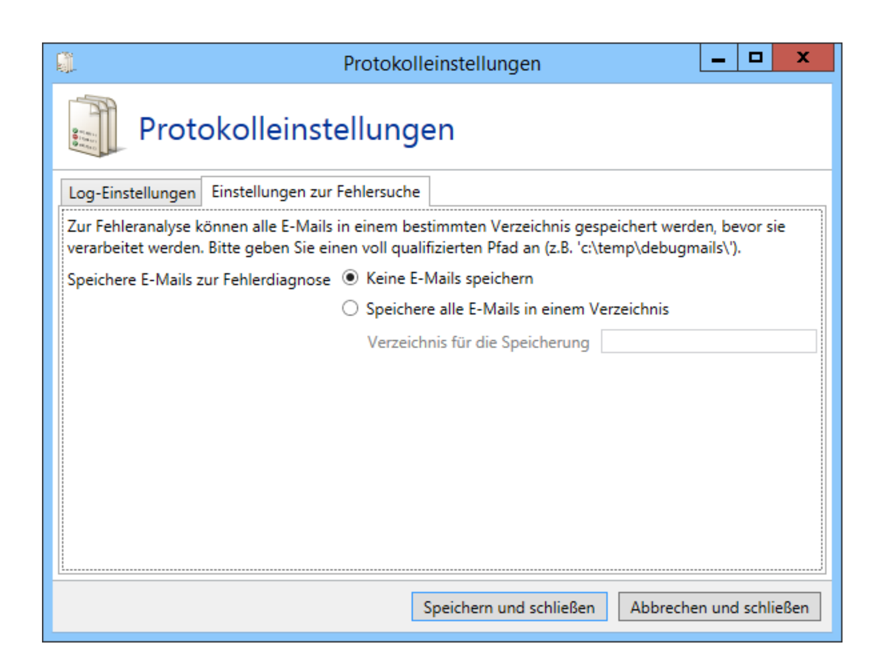


Bild 155: Speichern Sie zur Fehlerdiagnose den E-Mail-Verkehr auf der Festplatte



Beachten Sie, dass das Speicherung aller E-Mails auf der Festplatte einen hohen Platzbedarf haben kann und starke Leistungseinbußen des Servers nach sich ziehen kann. Nutzen Sie diese Funktion deshalb nur zur Fehlerdiagnose und schalten Sie sie danach wieder ab.

Geblockte IP-Adressen

Wie bereits erwähnt, sperrt das Mail Gateway nach Erhalt einer Spam-E-Mail das einliefernde Gateway standardmäßig für 30 Minuten aus. Falls aus Versehen eine vertraute IP-Adresse in diese Blacklist aufgenommen wird, so können Sie hier die Liste der gesperrten Gateways löschen (Bild 156).

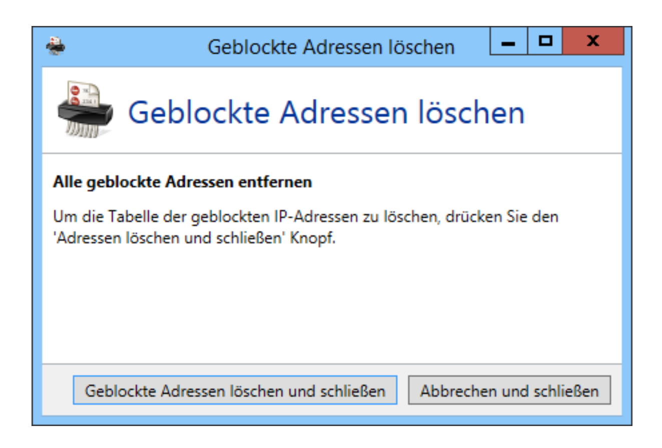


Bild 156: Löschen Sie geblockte IP-Adressen über diesen Dialog

Berechtigungen korrigieren

Falls die Dateisystemberechtigungen Ihres Mail Gateway durch z.B. Drittprogramme so verändert wurden, dass die Funktion eingeschränkt wird, können Sie das hier korrigieren. Es können Berechtigungen im Dateisystem (Bild 157) sowie auf der verwendeten Datenbank (Bild 158) korrigiert werden.

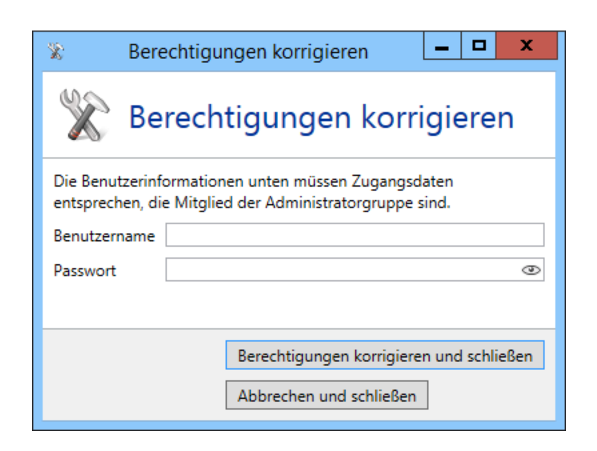


Bild 157: Lassen Sie Berechtigungen im Dateisystem korrigieren

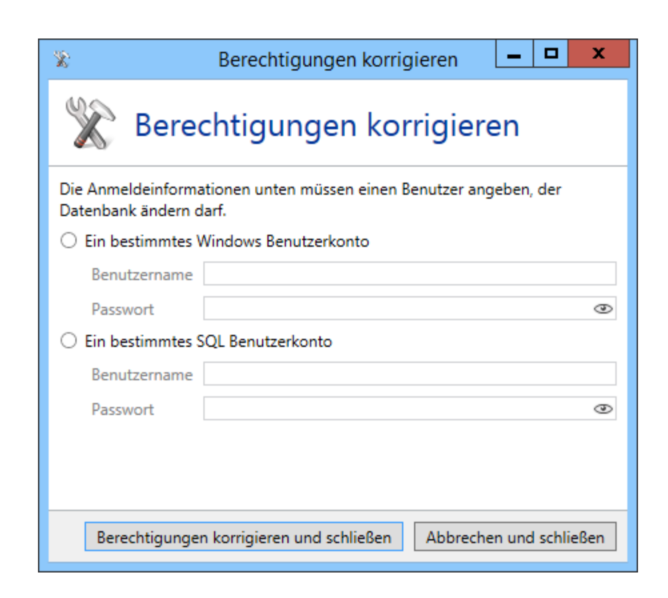


Bild 158: Lassen Sie Berechtigungen in der Datenbank korrigieren

10. Das Web Portal

Das Web Portal ermöglicht Ihren Kommunikationspartnern das übertragen großer Dateien an interne Benutzer. Für diese Funktion muss der **Large File Transfer** lizenziert sein.

Large File Transfer

Wenn Sie die Funktion **Large File Transfer** lizenziert haben können Ihre Benutzer einem externen Kommunikationspartnern die Möglichkeit geben Ihnen Dateien zu übermitteln, die zu groß für die Übertragung per E-Mail sind. Der interne Benutzer schickt dafür über das Outlook Add-In einen Link an den Empfänger, den dieser dann verwenden kann um Dateien zu übertragen.

Hat Ihr Kommunikationspartner eine Einladung für den Large File Transfer bekommen, so kann er über das Web Portal dem Absender auf sichere Art und Weise eine oder mehrere Dateien zukommen lassen (Bild 159).

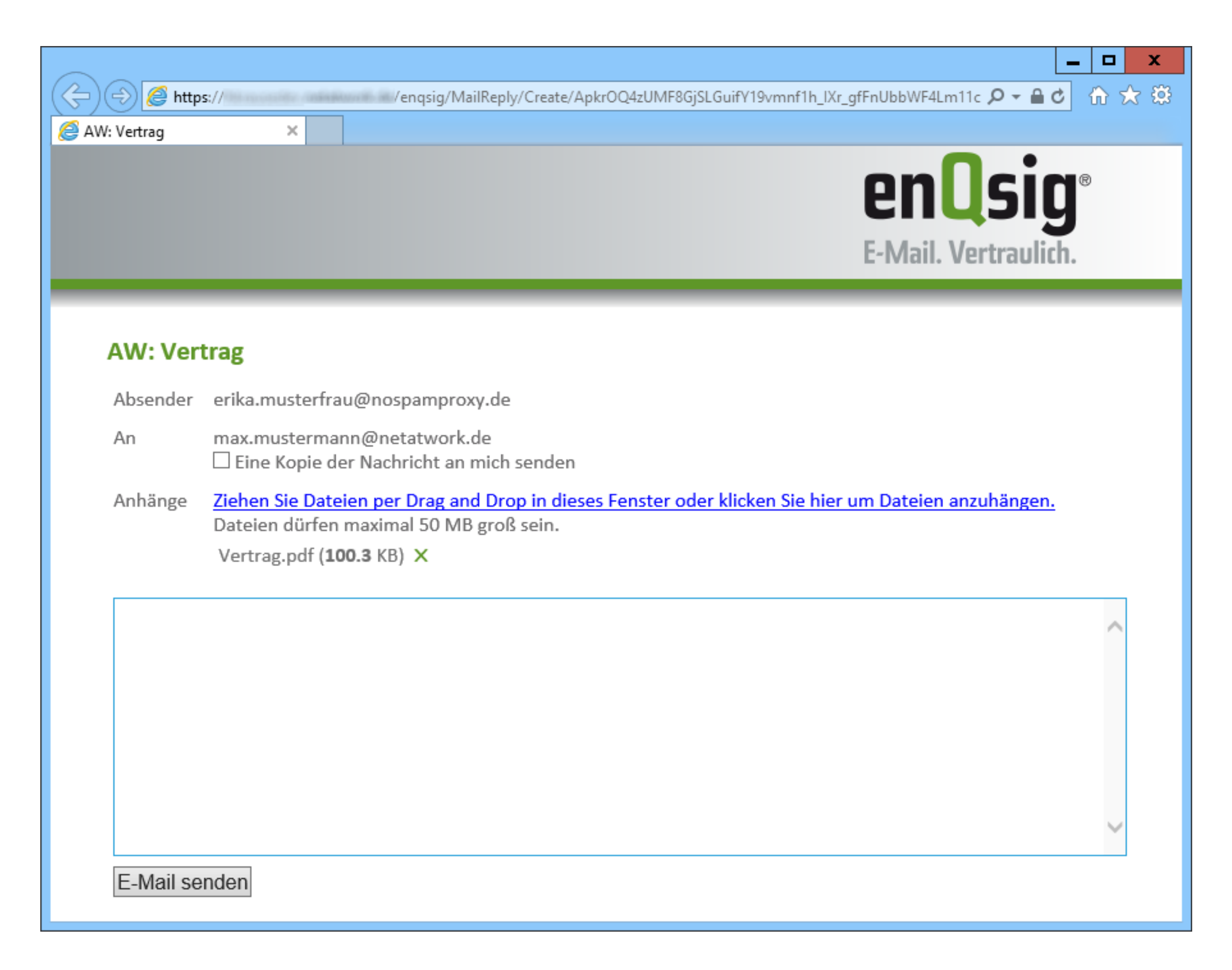


Bild 159: Dateien sicher übertragen über das Web Portal

Empfänger und Betreff sind festgelegt und können nicht geändert werden. Es ist dem Kommunikationspartner möglich, neben angehängten Dateien auch noch eine Nachricht zukommen zu lassen.

Je nach Konfiguration werden Dateien entweder direkt an die E-Mail angehängt, oder sie werden den Empfängern über den Large File Transfer bereitgestellt. Die Schwellwerte hierfür, sowie die maximale Größe pro Anhang kann vom Administrator festgelegt werden.

11. Anhang

Mehrfach verwendete Einstellungen in der Konfiguration

Einige Einstellungen werden in der Konfiguration mehrmals verwendet. Um die Lesbarkeit des Handbuchs zu erhöhen, werden diese hier ausführlich erläutert und bei der eigentlichen Verwendung in den unterschiedlichen Konfigurationen auf dieses Kapitel verwiesen. Dadurch werden immer wiederkehrende Erläuterungen vermieden.

Passwörter

Passwörter können in der Oberfläche in den folgenden Arten ausgeführt sein.

- **Einfache Passworteingabe**
  Die einfache Passworteingabe ist die häufigst verwendete Passworteingabe. Sie bietet die Funktion das Passwort durch ein Klick auf das Auge-Symbol am Ende der Eingabe kurzzeitig anzuzeigen. Die Anzeige unterstütz bei der Eingabe sowie bei der Fehlersuche. Diese Eingabe wird bei allen Eingaben benutzt, bei denen der Administrator zuvor auch selbst das Passwort eingeben hat.
- **Doppelte Passworteingabe**
  Bei der doppelten Passworteingabe muss zweimal das selbe Passwort eingegeben werden. Die Eingabe wird bei sehr sensiblen Passworten verlangt, deren Falscheingabe unbedingt vermieden werden soll. Die doppelte Passworteingabe kann wie die einfache Passworteingabe durch einen Klick auf das Auge-Symbol eingesehen werden. Diese Eingabe wird z.B. beim Schutz der sensiblen Daten des Gateways verwendet.
- **Passworteingabe ohne spätere Ansicht**
  Hier wird das Passwort nicht im Dialog angezeigt, sondern nur ein Hinweis ob ein Passwort bereits eingegeben wurde oder nicht. Der Administrator kann das Passwort dann gegenenfalls löschen oder auf einen neuen Wert setzen. Diese Art der Eingabe stellt sicher, dass durch dritte eingegebene Passworte nicht nach der Eingabe über die Oberfläche einsehbar sind. Um Schreibfehler zu vermeiden wird die verdeckte Eingabe immer als doppelte Passworteingabe ausgeführt. Diese Eingabe wird z.B. in den Verschlüsselungspassworten der externen Partner verwendet.

Auswahl von Zertifikaten

Bei der Auswahl von Zertifikaten erscheint der Dialog mit dem Titel **Wählen Sie ein Zertifikat aus** (Bild 160).

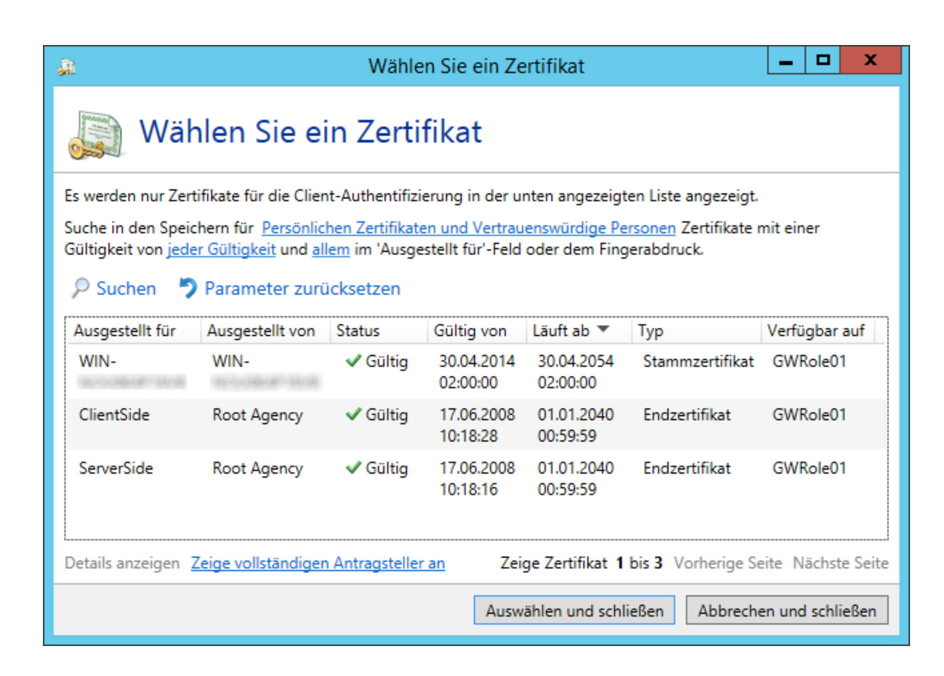


Bild 160: Die Liste der verfügbaren Zertifikate

Dabei werden Ihnen je nach dem in welchem Bereich Sie diese Zertifikate auswählen möchten, Zertifikate für die folgenden Verwendungszwecke angezeigt.

- **E-Mail-Authentifizierung**
  Ein Zertifikat, das dazu genutzt wird, den Versender einer E-Mail zu identifizieren.
- **Server-Authentifizierung**
  Ein Zertifikat, das dazu benutzt wird, einen Server eindeutig zu identifizieren.
- **Client-Authentifizierung**
  Ein Zertifikat, das dazu benutzt wird, einen Rechner, der sich mit einem Server verbinden will, eindeutig zu identifizieren.

Hier werden alle Zertifikate aus dem Zertifikatsspeicher der lokalen Maschine, das ist die Maschine, auf der die zu konfigurierende Rolle läuft, angezeigt. Wählen Sie das gewünschte Zertifikat aus und klicken Sie danach auf **Auswählen und schließen** um das gewählte Zertifikat zu nutzen, oder kontrollieren Sie vorher mit **Zertifikatsdetails anzeigen** alle Details des ausgewählten Zertifikats.



Einige Zertifikate, z.B. für De-Mail, sind durch identische Einträge im Feld **Ausgestellt für** schwer zu unterscheiden. Um diese Zertifikate zu unterscheiden, wählen Sie die Funktion **Zeige vollständigen Antragsteller an**. Dadurch wird der Antragstellername jedes Zertifikats ohne Kürzungen angezeigt.

Sicherung und Wiederherstellung

Um das Net at Work Mail Gateway im Falle eines Systemausfalls wiederherzustellen, ist es notwendig, alle für den Betrieb notwendigen Daten regelmäßig zu sichern.

Betriebssystem, Treiber und Software

Die Sicherung des Windows Betriebssystems sollten Sie mit erprobten Programmen durchführen. Da das Net at Work Mail Gateway sehr wenige Abhängigkeiten mit dem Betriebssystem selbst hat, ist es nach einem Ausfall auch möglich, den Ersatzserver frisch zu installieren. Wägen Sie daher ab, ob eine Neuinstallation des Betriebssystems und dessen Einstellungen und der Programme oder die Wiederherstellung der geeignete Weg ist.

Bei der Neuinstallation sollten Sie die bisher installierten Produkte und Einstellungen dokumentieren und die Datenträger vorhalten.

Weitere Informationen finden Sie in den Online Handbüchern und Anleitungen von Microsoft zu Windows Server und NTBACKUP.

Lizenzen des Net at Work Mail Gateways

Ihre Lizenz liegt als Datei auf dem Server im Verzeichnis

```
%ProgramData%\Net at Work Mail Gateway\Configuration\License.xml
```

und kann über ein normales Backup problemlos gesichert werden. Sie können die XML-Datei auch zusätzlich in einen sicheren Ordner kopieren. Die Datei ist auch im Betrieb nicht gesperrt und wird nicht beschrieben.

Konfigurationsdateien der Rollen

Die Konfiguration des Net at Work Mail Gateways wird in einer XML-Datei auf dem Server selbst gespeichert. Auch diese Datei kann mit einer handelsüblichen Backup Software ohne Probleme gesichert werden.

Allerdings schreibt das Gateway diese Datei bei Veränderungen der Konfiguration zurück, so dass hier ein Konflikt beim zeitgleichen Backup auftreten kann.

Das Net at Work Mail Gateway legt während des Schreibens der Konfiguration die neue Datei als temporäre Datei an, benennt die originale Datei in z.B. „GatewayRole.config.backup“ und benennt erst danach die temporäre Datei in „GatewayRole.config“ um. Bei einer normalen dateibasierten Sicherung haben Sie daher immer entweder die aktuellste Kopie oder die kurz zuvor geänderte Version der Konfiguration gesichert.

Es ist ratsam, auch vor größeren Änderungen an der Konfiguration diese Datei zu kopieren, um einfach zu dem vorherigen Stand zurückkehren zu können.

Die Konfigurationsdateien aller Rollen in der Standardkonfiguration werden nachfolgend aufgelistet. Sollten Sie das Net at Work Mail Gateway in einem anderen Pfad installiert haben oder von einer

früheren Version des NoSpamProxys das Programm aktualisiert haben, so muss der Pfad entsprechend angepasst werden.

- **Gateway Rolle**
  `%ProgramData%\Net at Work Mail Gateway\Configuration\GatewayRole.config`
- **Intranet Rolle**
  `%ProgramData%\Net at Work Mail Gateway\Configuration\IntranetRole.config`
- **ServerManagement Service**
  `%ProgramData%\Net at Work Mail Gateway\Configuration\ManagementService.config`

Datenbanken des Net at Work Mail Gateways

Das Net at Work Mail Gateway speichert die meisten Informationen in mehreren SQL-Datenbanken ab, die Sie ebenfalls sichern sollten. Die Rollen des Net at Work Mail Gateways verwenden dabei folgende Datenbanken:

- **Gateway Rolle**
  `NoSpamProxyDB`
- **Intranet Rolle**
  `NoSpamProxyAddressSynchronization`

Wenn das Gateway Ihren bestehenden Standard oder Enterprise SQL Server nutzt, können Sie dort mit dem Enterprise Manager eine periodische Sicherung aller Datenbanken konfigurieren. Beim Einsatz der SQL Server Express Edition müssen Sie manuell mit einem Skript die Datenbank sichern und bei Bedarf wieder herstellen.

Sichern Sie die Datenbanken über die Kommandozeile mit folgendem Befehl:

```
osql -S (local)\NOSPAMPROXYDB -E -Q "BACKUP DATABASE NoSpamProxyDB TO DISK =
'c:\nospamproxydb.bak'"
```

Diese Zeile sichert die Datenbank in eine Datei, ohne die Datenbank dazu herunter zu fahren. Sie sollten daher prüfen, ob Sie einen entsprechend angepassten Aufruf mit dem Windows Taskplaner als regelmäßige Aufgabe einplanen.



Bitte ersetzen Sie den im Beispiel für Backup und Wiederherstellung zweimal angegebene Datenbanknamen `NOSPAMPROXYDB` durch einen der vier oben angegebenen Datenbanknamen, um die jeweilige Datenbank zu sichern bzw. wiederherzustellen.

Die Rücksicherung erfolgt mit folgender Zeile:

```
osql -S (local)\NOSPAMPROXYDB -E -Q "RESTORE DATABASE NoSpamProxyDB FROM DISK
= 'c:\nospamproxydb.bak' WITH FILE= 1, NOUNLOAD, REPLACE "
```

Die Datenbank muss aber dazu schon bestehen.



Da der SQL-Server die Datenbanken selbst permanent geöffnet hält, können diese nicht über eine normale Sicherung der Dateien wie zum Beispiel über NTBACKUP erfasst werden.

Fehlersuche

Das Net at Work Mail Gateway beruht auf einer sehr einfachen Funktionsweise. Seine Implementierung als SMTP-Proxy verbindet die Vorteile dieses Prinzips mit der Einfachheit des Betriebs. Trotzdem kann es sein, dass das Gateway nach der Installation nicht so funktioniert, wie Sie es erwartet haben. Die häufigsten Fehler und Möglichkeiten zum Test beschreiben wir hier.

Support durch E-Mail

support@nospamproxy.de

Bitte fügen Sie folgende Informationen Ihrer E-Mail bei:

- **Ihre Kundennummer**
  Wir erfassen und pflegen alle Supportfälle in einem Support System. Ihre Kundenummer ist der Schlüssel, damit wir Supportanfragen eindeutig zuordnen können. Sie haben Ihre Kundennummer bei der Anforderung der Testlizenz oder dem Erwerb einer Lizenz erhalten. Sollte Sie Ihre Kundennummer nicht zur Hand haben, können Sie diese auch in der Lizenzdatei nachschlagen. Die Kundennummer, in unserem Beispiel die „C12345“, liegt in einem mit „ContactNumber“ benannten Bereich: `<field name="ContactNumber">C12345</field>` Sie können diese Nummer ebenfalls als Kundennummer angeben.
- **Die Konfiguration des Net at Work Mail Gateways**
  Die Lage der Konfigurationsdateien im Dateisystem wird im Abschnitt Konfigurationsdateien der Rollen beschrieben. Bitte hängen Sie diese, vor allem aber die Konfigurationsdatei der Gateway Rolle, an die E-Mail für unser Support Team an.
- **Netzwerkplan und Ihre Planung**
  Sofern Sie eine Beschreibung Ihrer Umgebung haben, hilft uns diese beim Verständnis, wie Sie das Net at Work Mail Gateway nutzen wollen. Besonders interessant ist dabei Ihre SMTP-Domänen, die IP-Adressen des internen E-Mail-Servers und wie Sie Ihre E-Mails aus dem Internet erhalten und versenden. Auch Informationen über Firewalls in den Übertragungswegen sind sehr hilfreich.
- **Informationen über Ihre Internetanbindung**
  Um das Net at Work Mail Gateway einzusetzen, müssen Sie Ihre E-Mails per SMTP empfangen. Ein Zugriff von extern auf ihr System über Port 25/TCP muss daher möglich sein. Welche Komponenten stehen zwischen dem Mail Gateway und dem Internet? Ein Router mit Port Filter und NAT oder eine vollwertige Firewall?
- **Informationen über den Server**
  Welches Betriebssystem und Service Packs haben Sie installiert? Haben Sie Portfilter oder eine Firewall auf dem Server aktiviert?
- **Fehlerbeschreibung**

Bitte beschreiben Sie möglichst genau, welchen Fehler Sie haben bzw. welche Funktion nicht gegeben ist.

Wir versuchen Ihnen schnellstens zu helfen. Bitte lesen Sie dennoch die folgenden Hinweise, um häufige Fehler zu erkennen und selbst zu beheben.

Das Net at Work Mail Gateway kontrollieren

Der erste Blick sollte der Management Oberfläche des Net at Work Mail Gateways gelten. Der Statusbildschirm auf der Überblicksseite gibt Ihnen sehr schnell einen Überblick über ihr System. Sie können hier unmittelbar sehen, ob alle Einstellungen fehlerfrei eingetragen sind (Bild 161).

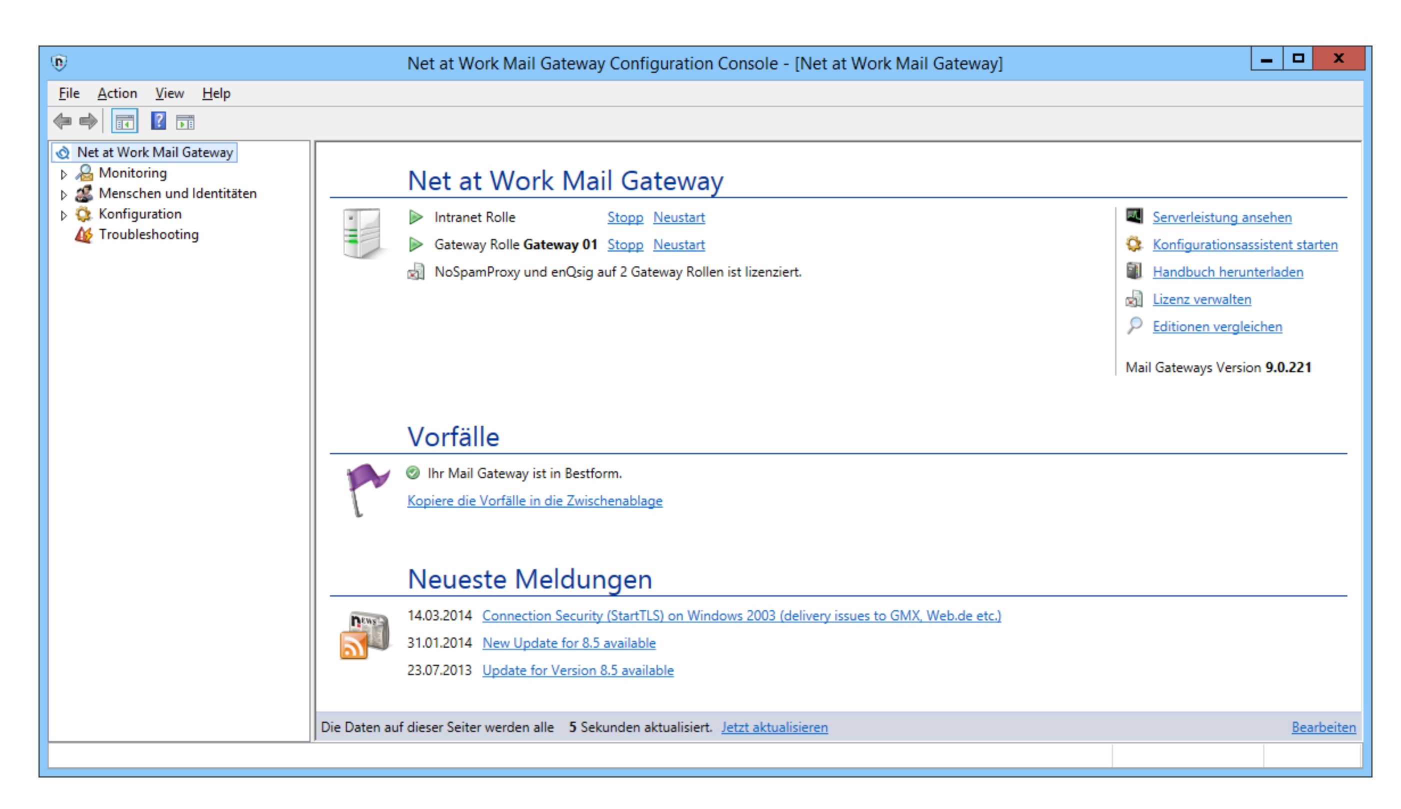


Bild 161: Die Übersicht zeigt eine vollständige Konfiguration des Net at Work Mail Gateways an

Kontrollieren Sie bitte die folgenden Punkte um Fehlerursachen zu finden.

- **Sind alle Rollen gestartet?**
  Alle Rollen sollten den Status „gestartet“ haben. Sie können die Rollen auch über die Oberfläche starten.
- **Werden Fehler angezeigt?**
  Fehler in der Konfiguration einer Rolle werden in der Übersicht über das Net at Work Mail Gateway angezeigt (Bild 162). Fehler sollten in einem vollständig konfigurierten Gateway immer beseitigt werden.
- **Werden Warnungen angezeigt?**

Warnungen sind ähnlich zu betrachten wie Fehler, mit dem Unterschied, dass Warnungen unter bestimmten Bedingungen durchaus auftreten können. Gehen Sie Warnungen genauso wie Fehlern auf den Grund und wägen Sie ab, ob die Warnung durch Ihre beabsichtigte Konfiguration des Net at Work Mail Gateways hervorgerufen wird oder besser behoben werden sollte.

- **IP-Adressen und Ports**
  Kontrollieren Sie, ob die Gateway Rolle des Net at Work Mail Gateways auf den richtigen IP-Adressen und Ports Verbindungen annimmt.
- **Werden überhaupt E-Mails übertragen?**
  Auf dem Statusschirm erkennen Sie die Anzahl der Verbindungen und übertragenen E-Mails als auch die Datenmenge. Stehen hier alle Werte auf 0, dann erhält das Net at Work Mail Gateway keine E-Mails. Die gleichen Werte können Sie mit den Windows Leistungsindikatoren auslesen.
- **Meldungen im Ereignisprotokoll**
  Das Net at Work Mail Gateway zeigt Ihnen in der Windows-Ereignisanzeige Fehlermeldungen, die eine Funktion behindern.

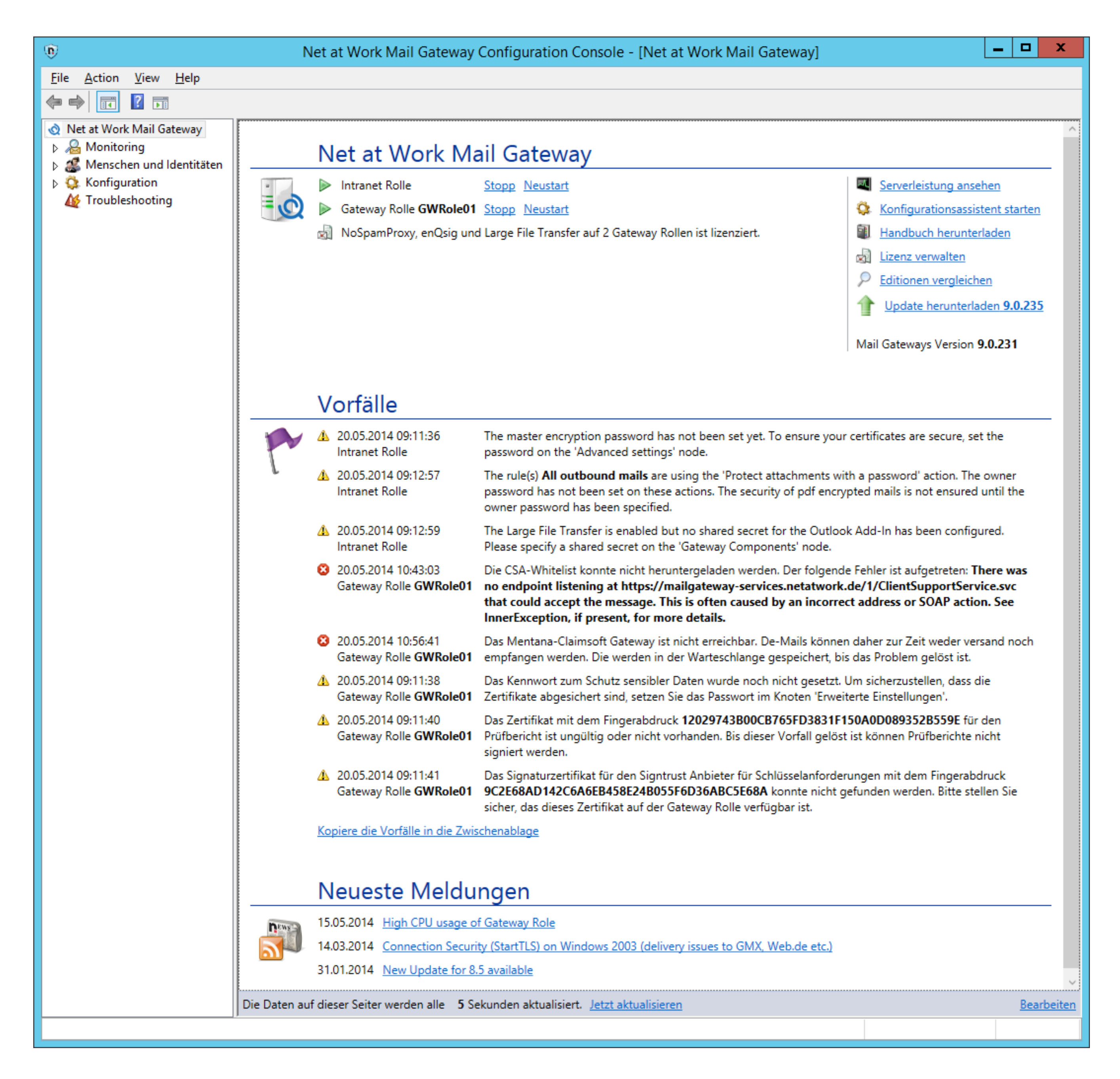


Bild 162: Fehler in den Konfigurationen des Net at Work Mail Gateways

Net at Work Mail Gateway testen

Die Basisfunktionen des Net at Work Mail Gateways lassen sich mit zwei Programmen testen, die ein Bestandteil von Windows sind:

- **TELNET**
  Der Versand einer E-Mail per SMTP ist sehr einfach und kann mit TELNET auch von Hand erfolgen.

- **NSLOOKUP**
  Dieses Programm dient zur Fehlersuche im Bereich der Namensauflösung. Das Mail Gateway nutzt DNS intensiv, z.B. um RBL-Listen abzufragen oder Zertifikate auf Gültigkeit zu überprüfen.

TELNET

Wenn ein E-Mail-Server eine E-Mail an einen anderen E-Mail-Server sendet, so erfolgt dies über TCP/IP über den Port 25. Diese Kommunikation können Sie mit TELNET auch manuell durchführen und dabei sehr gut das Verhalten des entfernten E-Mail-Servers oder des eigenen Net at Work Mail Gateways testen. Eine E-Mail per SMTP senden Sie einfach mit dem Programm Telnet. Dazu starten Sie den Verbindungsaufbau mit:

```
TELNET name-des-mailserver 25
```

Der E-Mail-Server sollte danach mit einer 220-Meldung den Verbindungsaufbau bestätigen. An dieser Stelle sind Sie nun mit Ihrem E-Mail-Server verbunden und können wie folgt eine E-Mail versenden. Geben Sie dazu folgende Befehle, immer gefolgt von einem „Return“ `<CR>`, ein. Warten Sie nach jedem Befehl auf die Bestätigung des E-Mail-Servers.

```
HELO name.des.absenderservers<CR>

MAIL FROM: mailadresse@absender.de<CR>

RCPT TO: mailadresse@zieldomäne.de<CR>

DATA<CR>
```

Ab nun geben Sie alles ohne weitere Rückmeldung des Servers ein:

```
Subject: Dies ist der Betreff<CR>

<CR>

Und hier ist der Body<CR>

. <CR>
```

Zum Abschluss enthält die letzte Zeile nur einen „Punkt“. Damit wird das Ende der E-Mail gekennzeichnet und der E-Mail-Server bestätigt den erfolgreichen Empfang der E-Mail. Mit dem Befehl `QUIT` wird die Verbindung zum E-Mail-Server geschlossen.

NSLOOKUP

Das Programm NSLOOKUP ist das Hilfsmittel zur Kontrolle der DNS-Namensauflösung. Starten Sie NSLOOKUP einfach in einem DOS-Fenster mit den entsprechenden Optionen.

Beispiele:

```
nslookup -q=A www.microsoft.com
```

Sie erhalten die Liste der IP-Adressen, welche die Webseite von Microsoft betreiben.

```
nslookup -q=MX netatwork.de
```

Sie erhalten die E-Mail-Server, welche E-Mails für die Domäne `netatwork.de` annehmen.

```
nslookup -q=A
```

```
nslookup -q=A 3.4.5.80.dnsbl.sorbs.net
```

Sie erhalten von der Liste „Sorbs“ die Information, dass dieser Servername die IP-Adresse `127.0.0.10` hat und damit auf der Liste der dynamischen IP-Adressen steht.

NSLOOKUP ist daher ein nützliches Hilfsmittel, um Fehler in der DNS-Konfiguration des Windows Server zu diagnostizieren.

Häufige Fehler und Ihre Ursachen

Das Net at Work Mail Gateway ist so entwickelt, dass nur die Schnittstellen gebunden und genutzt werden, die auch konfiguriert wurden. Gerade bei Systemen mit vielen Netzwerkkarten und IP-Adressen ist es daher wichtig, die Konfiguration gewissenhaft durchzuführen. Prüfen Sie daher folgende Einstellungen:

- **Port und IP-Adresse**
  Stellen Sie sicher, dass das Net at Work Mail Gateway wirklich auf den Adressen Verbindungen annimmt, die Sie ihm zugedacht haben. Vielleicht liegt nur ein Zahlendreher in der Konfiguration vor?
- **Telnet auf 127.0.0.1 Port 25 geht nicht**
  Beachten Sie hier, dass das Net at Work Mail Gateway nicht auf der localhost-Adresse arbeitet, wenn Sie den Dienst auf eine spezifische IP-Adresse gebunden haben.
- **Firewall**
  Gibt es auf dem Server eine Firewall oder einen Portfilter, die eine Verbindung zum Net at Work Mail Gateway auf TCP/IP-Ebene verhindern? Testen Sie die Erreichbarkeit des Gateways auf dem Server selbst mit einem TELNET Befehl auf die IP-Adresse. Damit schließen Sie eine externe Firewall testweise aus.
- **Andere Dienste?**
  Das Net at Work Mail Gateway versucht beim Start die angegebenen Schnittstellen einzubinden. Dies ist nicht möglich, wenn bereits ein anderes Programm die entsprechenden Schnittstellen eingebunden hat. Das Gateway zeigt dieses als Fehlermeldungen in der Ereignisanzeige und im Statusbild an.

Das Net at Work Mail Gateway ist standardmäßig relay-sicher und sehr gut gegen Missbrauch von außen als auch von innen geschützt. Dies bedeutet aber, dass Sie, ähnlich wie bei einer Firewall, genau die Funktionen erst frei schalten müssen, die Sie benötigen. Dazu gehören zwingend zwei Einstellungen:

- **Eigene Domänen**
  Sie müssen im Net at Work Mail Gateway die Liste der Domänen pflegen, die Sie intern betreiben. Anhand der Standardregeln nimmt das Gateway von extern nur E-Mails für diese Domänen an. Haben Sie hier keine Domänen gepflegt, so nimmt das Gateway keine E-Mails von extern

an. **Ausnahme:** Sie haben die Standardregeln verändert, so dass dieser Schutz nicht mehr gewährleistet wird.

- **Interne E-Mail-Server**
  Damit ausgehende E-Mails durch das Net at Work Mail Gateway zugestellt werden, müssen alle internen E-Mail-Server, von denen das Gateway E-Mails annehmen soll, in die Liste der internen E-Mail-Server eingetragen werden. Fehlen interne E-Mail-Server in der Liste, ist es nicht möglich von diesen Servern E-Mails zu versenden.

NoSpamProxy filtert nicht

Wenn NoSpamProxy korrekt installiert ist und E-Mails zwar durchgeleitet, aber keine blockiert werden, so kontrollieren Sie bitte folgendes:

- **Lizenz installiert**
  Wenn NoSpamProxy keine gültige Lizenz findet, dann werden alle Verbindungen auf „Durchreichen“ gestellt, d.h. die E-Mails werden ohne weitere Beachtung der Regeln durchgelassen.
- **Regeln**
  Kontrollieren Sie, ob Ihre Regeln Ihren Anforderungen entsprechen und die Filter und Grenzen passend eingestellt sind. Die Entscheidung „Durchreichen“ lässt alle E-Mails dieser Regel passieren. Auch die Reihenfolge der Regeln ist wichtig. Die Regeln werden sequentiell abgearbeitet. Die erste zutreffende Regel wird abgearbeitet und alle anderen werden nicht beachtet. Zum Testen empfiehlt es sich z. B. eine Regel am Anfang der Regelliste zu definieren, die E-Mails an eine bestimmte E-Mail-Adresse abweisen. Dieses könnte man z.B. mit der richtigen Einstellung im Reiter „Kriterien“ erreichen. Eine Test-E-Mail an diesen Empfänger muss von NoSpamProxy abgelehnt werden. Wenn dies erfolgt, dann landet die IP-Adresse des Testsystems in der Blacklist und Sie wissen, dass NoSpamProxy im Prinzip schon funktioniert. Allerdings müssen Sie nun ihr Regelwerk noch einmal genauer untersuchen.
- **E-Mail Nachrichtenverfolgung**
  Detaillierte Informationen zum Ablauf einer E-Mail bietet Ihnen die Nachrichtenverfolgung. Jede E-Mail, die durch NoSpamProxy verarbeitet wurde, ist in der Nachrichtenverfolgung zu finden. Dort finden Sie auch sehr einfach die Regel und die Filter bzw. Aktionen, die auf einer E-Mail angewendet wurde, inklusive der Bewertung. Im Falle eines Fehlverhaltens oder Eintreffen eines „False Positive“-Ereignisses bzgl. der E-Mail-Abwicklung durch NoSpamProxy, sollten sich in der Nachrichtenverfolgung ausreichende Hinweise diesbezüglich befinden.



Achten Sie bei der Kontrolle der E-Mails in der Nachrichtenverfolgung besonders auf die korrekte Richtung der E-Mail (ein- oder ausgehend).

Das Net at Work Mail Gateway lehnt alle eingehenden E-Mails ab

Das Net at Work Mail Gateway ist standardmäßig „relay-sicher“ und sehr gut gegen Missbrauch von außen als auch von innen geschützt. Dies bedeutet aber, dass Sie, ähnlich wie bei einer Firewall, genau die Funktionen erst frei schalten müssen, die Sie benötigen. Dazu gehören zwingend zwei Einstellungen:

- **Lokale E-Mail-Domänen**
  Sie müssen in dem Gateway die Liste der Domänen pflegen, die Sie intern betreiben. Anhand der Standardregeln nimmt es von extern nur E-Mails für diese Domänen an. Haben Sie hier keine Domänen gepflegt, so nimmt das Gateway keine E-Mails von extern an. **Ausnahme:** Sie haben die Standardregeln verändert, so dass dieser Schutz nicht mehr gewährleistet wird.

Wenn das Net at Work Mail Gateway externe E-Mails ablehnt, dann erstellt der E-Mail-Server, der versucht die E-Mail zuzustellen, eine Unzustellbarkeitsmeldung. Sie selbst können mit der TELNET-Testmethode ebenfalls eine E-Mail von extern an das Gateway übermitteln und die Meldung des Net at Work Mail Gateways ablesen, die den Grund für die Ablehnung nennt. Des Weiteren bietet Ihnen auch hier die Nachrichtenverfolgung ein hilfreiches Werkzeug zur Fehlereinkreisung.

SQL-Datenbank steht nicht zur Verfügung

Wenn Sie in den Regeln als Empfängerkriterium die Lokalen Benutzer ausgewählt haben, damit E-Mails an ungültige E-Mail-Adressen abgewiesen werden, lehnt das Net at Work Mail Gateway die E-Mail temporär ab, sobald er auf die SQL-Tabelle nicht zugreifen kann. Stellen Sie sicher, dass der SQL-Server Dienst ordnungsgemäß gestartet ist und das Gateway fehlerfrei auf die Datenbank zugreifen kann. Fehlermeldungen finden Sie unter anderem in der Ereignisanzeige des Net at Work Mail Gateways und in der Übersichtseite.

NoSpamProxy findet keine Viren

NoSpamProxy kann sowohl eingehende als auch ausgehende E-Mails auf virenverseuchte Anhänge prüfen und je nach Einstellung die komplette E-Mail ablehnen oder nur die Anhänge entfernen. Damit NoSpamProxy E-Mails mit Anhängen auf Viren überprüfen kann, müssen zwei Faktoren erfüllt sein:

- **Installierter Virenscanner**
  Auf dem NoSpamProxy-Server muss ein beliebiger Virenscanner installiert sein, der in Echtzeit die Zugriffe auf das Dateisystem überwacht und den Versuch, eine virenverseuchte Datei abzuspeichern, unterbindet.
- **Aktion „Dateibasierter Virusscanner“ muss eingebunden sein**
  Diese Aktion ist standardmäßig nicht mit eingebunden, da diese Aktion nur in Verbindung mit einem installierten Virenscanner einen Sinn ergibt. Da NoSpamProxy nicht feststellen kann, ob ein Virenscanner installiert ist, möchten wir Sie nicht in trügerischer Sicherheit wiegen. Um die Funktion eines Virenschutzes zu nutzen, müssen Sie daher einen dateibasierten Virenscanner installieren und dann die Aktion in die entsprechenden Regeln einbinden. Die Funktion des dateibasierten Virenscanners können Sie prüfen, in dem Sie den EICAR-Testvirus über die Seite http://www.eicar.com/ herunter laden oder sich zusenden lassen.

Smartcard nicht per RDP verwaltbar

Wenn Sie Zertifikate von einer Smartcard einsetzen, können Sie die Smartcard in einer RDP-Sitzung nicht verwalten. Das funktioniert nur in einer Sitzung direkt auf dem Host. In virtuellen Umgebungen basierend auf Hyper-V muss zum Beispiel der SCVMM Admin benutzt werden, in VMware Umgebungen der VMware Admin.

Exchange-Management-Konsole startet nicht mehr

Wenn das Net at Work Mail Gateway und Exchange 2010 auf demselben Server installiert sind, funktioniert die Exchange-Management-Konsole nicht mehr ordnungsgemäß. Der Grund hierfür ist das .NET Framework 4.0. Die Exchange-Management-Konsole benötigt das .NET Framework in der Version 2.0, die NoSpamProxy Management-Konsole hingegen arbeitet ausschließlich mit der Version 4.0.

Damit standardmäßig die richtige .NET Framework Version verwendet wird, legt das Net at Work Mail Gateway eine Umgebungsvariable mit dem Namen "COMPLUS_ApplicationMigrationRuntimeActivationConfigPath" an. Diese Variable verweist auf einen Pfad in dem eine Konfigurationsdatei mit den entsprechenden Einstellungen gespeichert ist. Beim Aufruf jeglicher MMCs wird die entsprechende Variable, und somit die Konfigurationsdatei, verwendet. Beim Öffnen der Exchange MMC verursacht dies die bekannten Probleme. Um die Exchange MMC wieder benutzen zu können, gibt es nur den folgenden Workaround: Die Umgebungsvariable wird dauerhaft gelöscht und die NoSpamProxy MMC muss über eine Batchdatei aufgerufen werden, in der die notwendigen Umgebungsvariable vorher definiert wird. Der Vorteil ist, dass die Umgebungsvariable in diesem Fall nur für Programme angewendet wird, die aus dem Kontext der Batchdatei aufgerufen werden.

Öffnen Sie über `Start -> Ausführen -> sysdm.cpl` die 'Erweiterten Systemeinstellungen' (Bild 163). Wählen Sie in der Karteikarte **Erweitert** / **Advanced** den Knopf **Umgebungsvariablen...** / **Environment Variables...**.

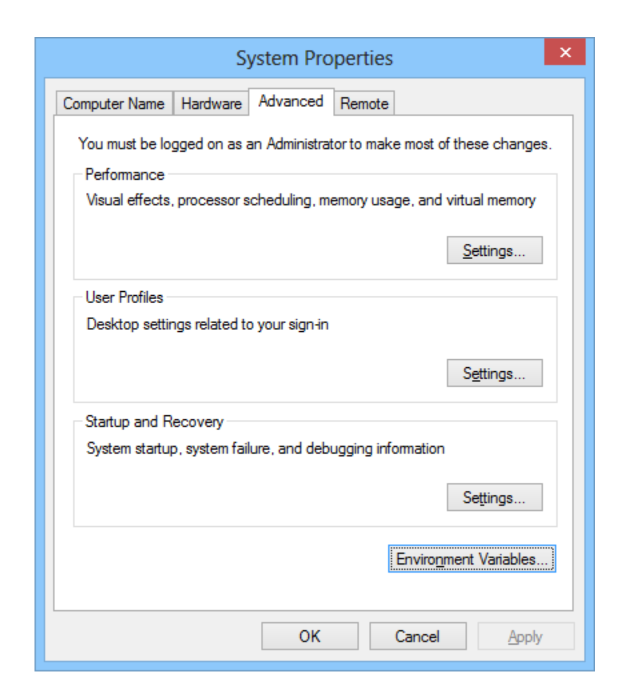


Bild 163: Die erweiterten Systemeinstellungen

Es öffnet sich das Fenster mit den 'Umgebungsvariablen' (Bild 164).

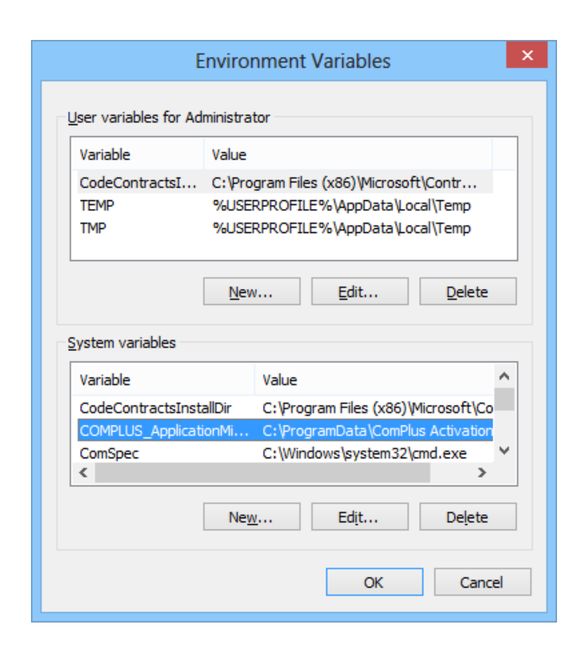


Bild 164: Die Umgebungsvariablen des Systems und des angemeldeten Benutzers

Wählen Sie im Abschnitt **Systemvariablen** den Eintrag `COMPLUS_ApplicationMigrationRuntimeActivationConfigPath` aus und klicken anschließend auf **Bearbeiten** / **Edit**. Kopieren Sie sich den Pfad, der im Feld **Wert** / **Value** steht, in die Zwischenablage. Anschließend löschen Sie den kompletten Eintrag. Schließen Sie die beiden offenen Dialoge jeweils mit **OK**. Öffnen Sie nun Notepad. Fügen Sie den gerade kopierten Pfad aus der Zwischenablage in Notepad ein. Zusätzlich fügen Sie bitte folgende Zeilen dazu (kopieren sie den folgenden Text hintereinander, ohne zusätzliche Leerschritte, in eine Zeile):

```
set COMPLUS_ApplicationMigrationRuntimeActivationConfigPath=mmc.exe "C:\
Program Files\Net at Work Mail Gateway\NoSpamProxy Management Console\
Net at Work Mail Gateway Configuration Console.msc"
```

Kopieren Sie den Pfad aus der Zwischenablage hinter die erste Zeile ein. Die Notepad-Datei sollte dann sinngemäß wie folgt aufgebaut sein (kopieren sie den folgenden Text hintereinander, ohne zusätzliche Leerschritte, in eine Zeile):

```
set COMPLUS_ApplicationMigrationRuntimeActivationConfigPath=C:\
ProgramData\ComPlus Activation Configurations\mmc.exe "C:\
Program Files\Net at Work Mail Gateway\NoSpamProxy Management Console\
Net at Work Mail Gateway Configuration Console.msc"
```



Bitte beachten Sie, dass die Darstellung der Batch-Datei durch automatische Zeilenumbrüche verfälscht wird. Der Befehl soll in einer Zeile stehen.

Passen Sie zum Schluss ggfs. den Pfad zur Net at Work Mail Gateway Configuration Console.msc an und speichern Sie anschließend den Notepad-Inhalt als NoSpamProxy-MMC.bat. Wenn Sie die BATCH-

Datei aufrufen, sollte sich die NoSpamProxy MMC erfolgreich öffnen lassen. Ab Windows 2008 mit aktiviertem UAC müssen Sie die Batchdatei jedoch stets als Administrator ausführen. Die Exchange MMC sollte sich nun ebenfalls fehlerfrei öffnen lassen.

Kontrolle der Verbindungen

Das Net at Work Mail Gateway arbeitet allein als SMTP-Proxy und in dieser Funktion ist NoSpamProxy auf die Erreichbarkeit der E-Mail-Server angewiesen. Es gibt mehrere Faktoren, die eine Erreichbarkeit des Gateway oder der E-Mail-Server verhindern. Ursachen könnten sein:

- **Fehlende Namensauflösung**
  Das Net at Work Mail Gateway nutzt je nach Einstellung die angegebene IP-Adresse oder den Servernamen der E-Mail-Server. Wird der Servername angegeben, so muss dieser über DNS auflösbar sein.
- **Falsch konfigurierte E-Mail-Server**
  Stellen Sie sicher, dass die E-Mail-Server auch Verbindungen vom Net at Work Mail Gateway annehmen. Gerade bei der Umstellung auf das Net at Work Mail Gateway kann es passieren, dass der E-Mail-Server nur E-Mails von dem bisherigen System annimmt. Des Weiteren muss beim ausgehenden E-Mail-Smarthost sichergestellt sein, dass das Gateway diesen Smarthost als Relay benutzen darf.
- **Verbaute Wege**
  Prüfen Sie, ob der das Net at Work Mail Gateway die Verbindung zu den anderen E-Mail-Servern aufbauen kann oder ob eine Firewall auf dem Net at Work Mail Gateway Server, dem Zielserver oder auf dem Weg dorthin eine Verbindung verhindert.

Um die Verbindung zu anderen Servern zu kontrollieren, können Sie das bereits beschrieben Programm Telnet nutzen. Folgende vier Tests sind durchführbar:

- **Simulation: Net at Work Mail Gateway zu internem E-Mail-Server**
  Starten Sie auf dem Server des Net at Work Mail Gateways das Programm `TELNET ip-adresse-des-internen-mailservers 25`. Ihr interner E-Mail-Server muss sich melden. Ist dies nicht der Fall, so müssen Sie die Netzwerkverbindung, Firewall-Regeln und den internen E-Mail-Server prüfen. Solange sich das Net at Work Mail Gateway nicht mit diesem internen E-Mail-Server verbinden kann, wird es auch keine Verbindung von Extern annehmen.
- **Simulation von extern**
  Starten Sie auf dem Net at Work Mail Gateway eine TELNET-Verbindung auf die als extern angegebene IP-Adresse des Servers und erstellen Sie eine E-Mail. Das Net at Work Mail Gateway muss diese Verbindung als „von extern“ erkennen. Sobald Sie den Envelope (HELO, MAIL FROM, RCPT TO, DATA) eingegeben haben, wird das Gateway die bisher ermittelten Daten prüfen und dann eine Verbindung zum internen E-Mail-Server aufbauen. Dies können Sie z. B. auch im Statusüberblick des Net at Work Mail Gateways sehen.
- **Weitergabe nach extern**
  Analog zur Verbindung nach intern muss das Net at Work Mail Gateway auch ausgehende E-Mails über einen E-Mail-Server versenden. Kontrollieren Sie mit `TELNET ausgehender-mailserver 25`, ob dieser Server vom Net at Work Mail Gateway erreichbar ist und E-Mails annimmt. Dieser E-Mail-Server muss dem Net at Work Mail Gateway erlauben, E-Mails in das Internet zu versenden, d.h. diesen Server als Relay zu nutzen. Ist dieser Server nicht erreichbar, so nimmt das Net at Work Mail Gateway keine Verbindungen mehr von intern an.

- **Verbindung von Intern**
  Dieser Test wird von Ihrem internen E-Mail-Server aus durchgeführt. Starten Sie hier `TELNET ip-adresse-von-Net-at-Work-Mail-Gateway 25`. Diesmal muss sich das Net at Work Mail Gateway melden und Ihre Testdaten annehmen. Im Message Tracking sollten Sie später erkennen, dass die E-Mail als ausgehend „Outbound“ eingestuft wurde.

Leistungsindikatoren

Die Leistungsindikatoren sind ein sehr vielseitiges Mittel, um Funktionen des Net at Work Mail Gateways in Echtzeit zu prüfen. Alle Leistungsindikatoren werden nicht über die Management Konsolen Oberfläche angezeigt, sondern sind über das Windows Programm „Zuverlässigkeits- und Leistungsüberwachung“ („perfmon.exe“) einsehbar. Dadurch können Sie die Arbeit des Net at Work Mail Gateways, genau wie die Ihres Betriebssystems, überwachen. Dieses kann auch automatisiert durch eine weitere Software, wie zum Beispiel den Microsoft System Center Operations Manager, geschehen. Sie können beispielsweise nachsehen, wie oft E-Mails mit einem bestimmten Schwellenwert (SCL) geblockt wurden oder welches Datenvolumen die eingehenden E-Mails aufweisen.



Die Leistungsindikatoren werden, bis auf wenige Ausnahmen im „Serverleistung“ Knoten, nicht in der Oberfläche angezeigt. Sie dienen eher zur automatischen Überwachung des Net at Work Mail Gateways durch Softwareprodukte Dritter.

Die für das Net at Work Mail Gateway zur Verfügung stehenden Werte sind unten aufgeführt. Die Namen der Leistungsindikatoren sind, unabhängig von der gewählten Sprache des Betriebssystems oder des Net at Work Mail Gateways, immer in englischer Sprache.

NoSpamProxy Globals

- Accepted mails
- Blocked connections
- Delivery failures
- Rejected at envelope level
- Rejected at body level

NoSpamProxy Network Utilization

- Bytes Sent
- Bytes Received
- Active inbound connections
- Active outbound connections

NoSpamProxy Assigned Spam Confidence Levels

- SCL lower than 0
- SCL between 0 and 0.9

- SCL between 1 and 1.9
- SCL between 2 and 2.9
- SCL between 3 and 3.9
- SCL between 4 and 4.9
- SCL between 5 and 5.9
- SCL between 6 and 6.9
- SCL between 7 and 7.9
- SCL between 8 and 8.9
- SCL between 9 and 10

NoSpamProxy Actions

- Number of times run
- Permanently blocked
- Temporarily blocked
- Active outbound connections

NoSpamProxy Performance

- Average Response Time
- Filter requests awaiting execution
- Average action execution time
- Average filter execution time
- Average filter queue time
- Pagefile usage

Einstellungen über die Konfigurationsdatei

Direkt Änderungen der Konfiguration können das Net at Work Mail Gateway in einen nicht mehr startfähigen Zustand versetzen.

Aktivieren der Option 'Zustellen von ungültigen E-Mails'

Kann das Net at Work Mail Gateway E-Mails aufgrund fehlerhaften Aufbaus nicht überprüfen, dann wird die E-Mail abgelehnt. Seit der Version 6.11 kann man dieses Verhalten abschalten.



Überlegen Sie gut, ob Sie diese Option aktivieren. Betroffene E-Mails können von der Gateway Rolle nicht auf Spam und Viren überprüft werden.

Um die Option zu aktivieren, öffnen Sie die Konfigurationsdatei der Gateway Rolle des Net at Work Mail Gateways. Der Pfad zu der Datei heißt im Allgemeinen `%ProgramData%\Net at Work Mail`

`Gateway\Configuration\GatewayRole.config`. Bitte beachten Sie, dass Sie die Datei erst abspeichern können, wenn der Dienst der Gateway Rolle beendet ist. Anderenfalls werden alle Änderungen verworfen.

Bitte suchen Sie in der Datei zunächst die folgenden Zeilen:

```
</outboundDispatcherConfiguration>
</netatwork.nospamproxy.proxyconfiguration>
```

Fügen Sie dort den folgenden Schlüssel ein:

```
<dispatchInvalidMails isEnabled="true" />
```

Die Zeilen sollten dann wie folgt aussehen:

```
</outboundDispatcherConfiguration>
<dispatchInvalidMails isEnabled="true" />
</netatwork.nospamproxy.proxyconfiguration>
```

Speichern Sie die Datei ab und starten Sie anschließend die Gateway Rolle wieder.

SMTP RFCs

Die meisten im Internet verwendeten Protokolle basieren auf Ideen und Vereinbarungen zwischen mehreren Personen, die nach einiger Zeit zum Standard deklariert wurden. Diese Dokumente tragen das Kürzel RFC (Request for Comment). In den Anfangszeiten des Internet haben mehrere Personen verschiedener Firmen und Institute an verschiedenen Projekten gearbeitet und in Ermangelung einer zentralen Koordinierungsstelle Ihre Überlegungen und Protokolldefinitionen zur Diskussion gestellt.

Das Net at Work Mail Gateway nutzt das Protokoll SMTP. Die Details, wie SMTP funktioniert und auf welche Aktion welche Reaktion zu erfolgen hat, ist in entsprechenden RFC-Dokumenten beschrieben.

Die folgende Liste zeigt die wichtigsten RFC-Dokumente:

- RFC1123 for important additional information
- RFC1893 und RFC2034 for information about enhanced status codes
- RFC:2821 Simple Mail Transfer Protocol (SMTP)
- RFC:2822 Internet Message Format
- RFC-2554, AUTH, Authentication
- RFC-3207, STARTTLS, Start transport layer security

SMTP Errorcodes

Alle Rückmeldungen, die ein SMTP Server an das andere System meldet, beginnen mit einer Nummer. Der Text hinter der numerischen Angabe ist optional, kann sich von E-Mail-Server zu E-Mail-Server ändern und wird von Programmen nicht ausgewertet; er dient lediglich als Hilfe für Administratoren bei der Fehlersuche.

SMTP Errorcodes werden in diesen RFCs beschrieben:

- RFC:2821 Simple Mail Transfer Protocol (SMTP)

- RFC:2822 Internet Message Format
- Q257186 XIMS: SMTP Reply Codes (RFC 821)
- Q257167 XIMS: SMTP Reply Code 451

Die Return Codes setzen sich wie folgt zusammen. Jeder Code ist dabei dreistellig. Die erste Ziffer gibt dabei die Klassifizierung der Meldung an:

- 1yz = ok
- 2yz = completed
- 3yz = intermediate ok (Zwischenbescheid)
- 4yz = transient negative (vorläufig negativ)
- 5yz = permanent negative

Die zweite Stelle definiert die Quelle der Meldung:

- x0z = Syntax
- x1z = Info
- x2z = Connection
- x3z/x4z = nicht definiert
- x5z = Mailsystem

Die am häufigsten anzutreffenden Fehlernummern werden hier noch einmal aufgeführt:

- 200 (nonstandard success response, see rfc876)
- 211 System status, or system help reply
- 214 Help message
- 220 <domain> Service ready
- 221 <domain> Service closing transmission channel
- 250 Requested mail Aktion okay, completed
- 251 User not local; will forward to <forward-path>
- 354 Start mail input; end with <CRLF>.<CRLF>
- 421 <domain> Service not available, closing transmission channel
- 450 Requested mail Aktion not taken: mailbox unavailable
- 451 Requested Aktion aborted: local error in processing
- 452 Requested Aktion not taken: insufficient system storage
- 500 Syntax error, command unrecognised
- 501 Syntax error in parameters or arguments
- 502 Command not implemented
- 503 Bad sequence of commands
- 504 Command parameter not implemented

- 521 <domain> does not accept mail (see rfc1846)
- 530 Access denied
- 535 SMTP Authentication unsuccessful/Bad username or password
- 550 Requested Aktion not taken: mailbox unavailable
- 551 User not local; please try <forward-path>
- 552 Requested mail Aktion aborted: exceeded storage allocation
- 553 Requested Aktion not taken: mailbox name not allowed
- 554 Transaktion failed

Um eine genauere Unterscheidung der einzelnen Fälle Fehlerzustände anhand der dritten Stelle zu erlauben, wurden erweiterte Statusmeldungen eingeführt. Sie dienen dazu mehr als 10 Unterschiedliche Statuscodes zurückzugeben.

Diese werden in dem folgenden RFC Dokument genauer definiert:

- Q256321 RFC 1893 (Q256321) for Enhanced Status Codes for Delivery Status Notification (DSN) messages

Die Rückmeldung eines Servers kann wie folgt aussehen:

```
250 2.1.0 user1@example.com....Sender OK
```

Hinter der dreistelligen Meldung 250 folgt die ausführliche Meldung 2.1.0.

SMTP Timeouts

Bei der Verbindung zwischen zwei Systemen kann es immer zu Verzögerungen bei der Verarbeitung kommen. Heutzutage ist eine überlastete Leitung selten die Ursache für Verzögerungen.

In der Regel muss der empfangende E-Mail-Server die Daten annehmen und abspeichern; hierfür benötigt er Zeit. Daher sendet er seine Statusmeldung erst nach dem Abschluss dieser Tätigkeiten.

Auch das Net at Work Mail Gateway nimmt eine E-Mail teilweise an, was einige Zeit beansprucht, um anhand der Regeln entsprechende Aktionen zu starten. Erst nach dem Abschluss erhält das einliefernde System eine Meldung, um mit der Übertragung fortzufahren oder die Verbindung zu unterbrechen.

Auch diese maximalen Wartezeiten sind in der RFC 2821- Simple Mail Transfer Protocol“ definiert.

Folgende Zeiten gelten als Empfehlung:

- **Erste 220 Meldung nach dem Verbindungsaufbau: 5 Minuten**
  Der Sender muss einen Unterschied zwischen einer nicht angenommenen Verbindung und einer verzögerten Antwort durch hohe Belastung unterscheiden können. Sehr häufig nimmt der TCP/IP-Stack eine Verbindung an; doch der SMTP Server verzögert die Versendung der 220 Nachricht bis das System die Verarbeitung weiterer E-Mails zulässt.
- **MAIL-Befehl: 5 Minuten**
  Nach spätestens 5 Minuten muss ein E-Mail-Server auf das „MAIL FROM“ geantwortet haben
- **RCPT-Befehl: 5 Minuten**

Nach spätestens 5 Minuten muss ein E-Mail-Server auf das „RCPT TO“ geantwortet haben.

- **DATA: 2 Minuten**
  Nach spätestens 2 Minuten muss ein E-Mail-Server auf den Befehl „DATA“ reagieren. Dies ist ein für das Net at Work Mail Gateway wichtiger Wert, da die Abarbeitung der Envelope Filter nicht länger dauern darf. Normalerweise antwortet dann der E-Mail-Server mit einem „354 Start Input“
- **Datenblock: 3 Minuten**
  Die Übertragung der eigentlichen E-Mail erfolgt mittels TCP/IP-Blöcken. Die Bestätigung eines Blocks darf nicht länger als 3 Minuten ausbleiben.
- **DATA Abschluss: 10 Minuten**
  Nach der Übertragung der E-Mail sendet der absendende E-Mail-Server eine letzte Zeile, die nur einen Punkt enthält und wartet auf die Bestätigung. Der empfangende E-Mail-Server hat bis zu 10 Minuten Zeit auf das Endesignal mit „250 OK“ oder einer anderen Meldung zu antworten. Diese Zeit hat daher auch das Net at Work Mail Gateway, um die E-Mail durch verschiedene Filter zu bewerten, durch Aktionen zu verändern und an den internen E-Mail-Server zuzustellen. Erst wenn der empfangende E-Mail-Server die eingehende E-Mail mit „250 OK“ quittiert, übernimmt dieser auch die Verantwortung für die weitere Zustellung. Das Gateway sendet diese Meldung erst dann, wenn der interne E-Mail-Server die E-Mail komplett angenommen hat. Das Net at Work Mail Gateway ist daher zu keinem Zeitpunkt für die weitere Übermittlung verantwortlich.
- **Empfängertimeout: 5 Minuten**
  Auch umgekehrt gibt es einen Timeout. Wenn der empfangende E-Mail-Server seine Antwort übermittelt hat, ist der Sender gefordert, die nächsten Befehle zu übermitteln. Bleibt die nächste Meldung jedoch aus, so sollte der Empfänger mindestens 5 Minuten warten, ehe die Verbindung unterbrochen wird.

Glossar

- **API**
  Programmierschnittstelle, damit andere Programme auf das eigene Software System zugreifen können. http://de.wikipedia.org/wiki/Programmierschnittstelle
- **C-Nummer**
  Die C-Nummer ist Ihre eindeutige Lizenz-Nummer. Sie hilft dem Support-Team von Net at Work, Ihre Anfragen schnellstmöglich zu bearbeiten.
- **CER**
  Dateiendung zur Kennzeichnung von Dateien, die öffentliche Zertifikate enthalten.
- **DER**
  Dateiendung zur Kennzeichnung von Dateien, die öffentliche Zertifikate enthalten.
- **FQDN**
  Voll qualifizierten Domänenname. Ein Computer mit dem Name „mailserver“ in der DNS Domäne „example.com“ besitzt als FQDN den Namen „mailserver.example.com“. http://de.wikipedia.org/wiki/FQDN#Fully_Qualified_Domain_Name_.28FQDN.29
- **Hacker / hacken**
  Im Bereich dieses Handbuchs werden als „Hacker“ Personen mit umfangreichem Grundlagenwissen über Computersicherheit bezeichnet, deren vorrangiges Ziel ein Eindringen in fremde Computersysteme ist. http://de.wikipedia.org/wiki/Hacker_(Computersicherheit)
- **OCSP - Online Certificate Status Protocol**

Ein Internet Protokoll, um den Status eines Zertifikats bei einem Validierungsdienst nachzufragen. Durch einen OCSP Dienst können z.B. ungültige Zertifikate schon vor Ablauf ihrer Gültigkeit als ungültig erklärt werden. http://de.wikipedia.org/wiki/Online_Certificate_Status_Protocol

- **Öffentliche Zertifikate**
  Öffentliche Zertifikate sind Zertifikate, die keinen privaten Schlüssel enthalten. Man kann mit diesen Zertifikaten nur verschlüsseln. http://de.wikipedia.org/wiki/Digitales_Zertifikat
- **Persönliche Zertifikate**
  Persönliche Zertifikate sind Zertifikate, die einen privaten Schlüssel und einen öffentlichen Schlüssel enthalten. Man kann mit diesen Zertifikaten Nachrichten signieren und Nachrichten entschlüsseln, die zuvor mit dem öffentlichen Schlüssel dieses Zertifikats verschlüsselt wurden. http://de.wikipedia.org/wiki/Digitales_Zertifikat
- **Platzhalter**
  Ein Platzhalter (oder Wildcard) bezeichnet reservierte Zeichen die zur Ersetzung durch andere Zeichen dienen. Das Sternchen '*' steht für beliebig viele (auch null) Zeichen. Beispiel: Eine suche nach 'max*' findet alle Worte die mit 'max' beginnen, also auch 'maximal', 'maximilian' usw. Eine Suche nach 'm?x' findet 'mix', 'mux', 'max', 'm4x' usw.
- **Signieren**
  Der Vorgang des Signierens bezeugt die Authentizität einer Nachricht, in dem mit Hilfe der privaten Schlüssels eine Prüfsumme über die Nachricht erstellt wird. Dann wird der öffentliche Teil des Zertifikats an die Nachricht angehängt und Sie zum Empfänger übertragen. Der Empfänger kann mit Hilfe des öffentlichen Schlüssels die Prüfsumme überprüfen.
- **P12**
  Dateiendung zur Kennzeichnung von Dateien, die private Zertifikate enthalten.
- **PFX**
  Dateiendung zur Kennzeichnung von Dateien, die private Zertifikate enthalten.
- **RFC**
  Technische und organisatorische Dokumente zur Festlegung der Kommunikationsstandards im Internet. http://de.wikipedia.org/wiki/Request_for_Comments
- **S/MIME**
  Standard für die Signatur und Verschlüsselung von einer MIME-gekapselten E-Mail durch ein asymmetrisches Kryptographiesystem. http://de.wikipedia.org/wiki/S/MIME
- **StartTLS**
  Ist ein Verfahren, um eine E-Mail-Verschlüsselung auf Transportebene einzuleiten. http://de.wikipedia.org/wiki/STARTTLS